THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

Ministry of Technology

BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS

Volume 02 of 03 - Annexure 2: Non Functional Requirements

Single Stage Two Envelopes Bidding Procedure

FOR THE

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

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

May 07, 2023

Table of Contents

List of Tables

2.1. Trust, Privacy and Security

The establishment and operation of the Foundational ID platform require putting in place an elaborate set of safeguards that fall under the heading of trust, privacy, and security. Collectively, these are intended to ensure that the system operates within the boundaries of the law, does not violate people's rights, and is protected from abuse, risks, and vulnerabilities so that it can earn the confidence of those who rely on it.

2.1.1. Trust

Paramount for the success of UDI is, earning the trust of all stakeholders that relies on it. This includes the citizens whose identity is managed by the UDI and the public and private sector entities who rely on UDI to authenticate and provide KYC data to carry out their operation. Hence it is of utmost importance UDI to pay due attention to build and retain the trust; this section details the important factors that the program needs to address.

No	Trust Element	Key Consideration
1.	**Registration Integrity**	This is a crucial element in the chain of trust. The registration process should ensure that only legitimate identities are able to enrol. ***Required Measures:*** i) Assurance of captured data integrity at the enrolment centres and during transmission to prevent alterations, substitutions, or other manipulations. ii) When using biometrics, controlling captured image quality as measured metrics such as fingerprints or ICAO face image quality , Iris as specified. The image quality must meeting the required standard as specified in the volume 2. iii) • Matching accuracy of ABIS, if used, in the backend system should be high enough that (together with deterrence) it can lead to practically zero duplicate enrolments.
2.	**Trusted Credential**	The digital credential as well as the physical proxy should be virtually impossible to fabricate outside the SL-UDI ID Process. ***Required Measures:*** i) Mature and consistent information security, certificate management, and encryption practices that leave no loopholes.

No	Trust Element	Key Consideration
		ii) Minimum security requirements for any medium that will carry the credential, such as smartcards or mobile phones.
3.	**Identity Assurance**	Relying parties need to be assured that the person conducting a transaction is who he claims to be and not someone who stole a legitimate identity. ***Required Measures:*** Strong authentication: multifactor or biometric 1:1 match.
4.	**Combating Malfeasance (Human Factors)**	Preventing the issuance of true-false identity, where a human operator could issue a genuine document for a false identity due to bribe or coercion. ***Required Measures:*** i) Supervised procedures and technology to limit the ability of enrolment agents to fabricate fake enrolment data (often by presenting the wrong sequence of fingers, or by mixing and matching fingers from multiple people, including their own as they reconstitute the 10-print). ii) Internal controls at the DRP/UDI to ensure that no single operator is capable of surreptitiously modifying or enrolling identity records without supervisor approval.
5.	**Data Protection and Security**	The public should be assured that their data at the UDI is protected against unauthorized access, including external (hacking), internal (rogue employee), as well as organized mission creep. ***Required Measures:*** i) Information security measures that emphasize strong information rights management. ii) Physical security measures to protect data centres. iii) Identity data segregation. iv) Enforced internal policy and procedures for access. v) Public policy on data use.

No	Trust Element	Key Consideration
6.	**Trust Model**	One of the critical aspects of the Foundational ID platform, is the technology for trusted communication. This includes enabling authentication for access to online services, digital signature for commitment and non-repudiation, and encryption to secure transmission of transactions. Not only technical measures have to be in place, but also clearly defined responsibilities and liabilities of the authority providing this trust (e.g., CA/CSP) should be set in a Legal Regulations/Act and/or Governance Model.
7.	**Country Regulations / Legal aspects**	This is covered in the below set of regulations and not limited to (Data Protection, Electronic transactions. Act, no. 19 of 2006, Cyber Security Bill)

Table 2.1 :Important Trust Factors

2.1.2. Privacy

Data privacy is challenging since it attempts to use data while protecting an individual's privacy preferences and personally identifiable information. Privacy is the ability of an individual, group, or individuals or entity to free itself from being observed information about them with due consent.

UDI generates sensitive data during enrolment and when it is used to enable the actions of its holder (audit trail of transactions). More precisely, UDI evokes privacy concerns primarily for the following reasons:

No	Element	Key Consideration
1.	**Enrolment Data**	The Foundational ID platform registration process requires the collection of significant amounts of personally identifying information (PII) for validation and vetting,
2.	**Central Database**	Central Database not only does a Foundational ID platform capture PII during enrolment, but it also consolidates that data into central repositories to guard against duplicative registration and to deliver identity services.
3.	**UDI Number allows data correlation**	The use of the Unique Identity Number as an administrative tool to manage identity evokes privacy concerns since it enables the linking of disparate information about an individual across databases.

No	Element	Key Consideration
		Required Measures: i) It should be a random number with no encoding intelligence or profiling information. ii) It should have checksums and mechanisms to detect whether a given number is in the format of UDI number. iii) It should have less guess-ability to prevent fraudulent usage of UDI number iv) It should have significant length to accommodate the population for next few decades. v) It should have flexibility to accommodate future requirement of allocation to the entities rather than individuals only.
4.	**Digital Audit Trail**	Over time, with the implementation of the SL-UDI it would become pervasive; it would enable a dominant number of the population's daily actions.

Table 1.2 : Reasons for Invoking Privacy Concerns

Protecting user data privacy is a key requirement for UDI and is of utmost importance for the overall success of the program. Hence the program needs to consider the measures outlined below to avoid any privacy concerns. The MSI should address the above concerns during the implementation of the project.

No.	Trust Element	Key Consideration
1.	**Legislation**	The systems should be in compliance with the of Data. Protection Act, No. 9 of 202 Several obligations have been imposed by this legislation on those who collect and process personal data ("Controllers" and "Processors") and a whole new set of rights have been given to citizens under this new legislation, which are known as "Rights of data subjects". UDI specific Legal Acts: Implement where necessary UDI specific legal acts to reiterate or introduce new bodies of legislation that explicitly provide privacy protection to people.

No.	Trust Element	Key Consideration
2.	**Access and Data Protection**	The protection of identity data and limiting its use, using technical measures: ***Required Measures:*** i) Data rights access management. ii) Anti-data retention measures (e.g. retention of audit trail data only for the period required by law for non-repudiation). iii) Use limitations.
3.	**Notice**	The system should comply with the following, i) Individuals' right to have noticed regarding the data gathered about themselves and the right to know how and for what purpose it will be used. This may be required by law, or it may be good practice for all e-ID processes (enrolment, use). ii) Clear, meaningful, and prominent notice when collecting identifying data (iconic plus information link).
4.	**Consent/ Choice**	The individual's right to consent to the collection and use of their personal data. *Refer Consent management in Vol 2 and annexure 1.*
5.	**Privacy by Design**	These include privacy-enhancing technologies and measures such as: i) Data minimization and proportionality: capture data in proportion to risk. ii) Identity data segmentation and segregation: e.g., store identifiers separately from PII. iii) Do-not-track (DNT). iv) Right to view. v) Pseudonymous, or anonymous transaction management (Trusted Agents).
6.	**Privacy Policy and Support Framework and Enforcement**	Implementation of program-specific (Foundational ID platform-wide), as well as specific applications privacy policy to create awareness and implant the importance of privacy.

No.	Trust Element	Key Consideration
		Meaningful legal instruments and mechanisms that provide sanctions for noncompliance. Enforcement is not necessarily limited to the scope of action of the Privacy Commissioner's Office.

Table 2.2 : Data Privacy Issues to Consider

2.1.3. Security

At a basic level, a Foundational ID Platform is an information system that is supposed to secure online human interactions. As such, in addition to the measures needed to build trust and respect privacy, as discussed above, the information system requires sound information security safeguards that mitigate against the risk of breach and other operational vulnerabilities, spanning areas of legislation, governance, technology, and operational control.

No.	Element	Key Consideration
1.	**User authentication and authorization**	An Identity Access Management (IAM) needs to be developed to manage users and permissions. The MSI shall ensure that the admin application is only accessible within the internal network. ***Authentication*** The application should be able to verify users. Users will be authenticated based on an identifier/secret pairing (A username/password combination). The authentication service has decoupled using JWT (Jason web token) tokens, and there is no persistent session between server and client. User access and executes services with JWT token. ***Authorization*** The application should be able to verify that it allowed users to have access to resources. Role-Based Access Control (RBAC) will be used to ensure the operation of the Foundational ID platform will be restricted and tightly controlled users with relevant permission levels. Domain logic rules that apply to specific functional scenarios will also adhere. Even though there are roles, it only restricts users' login to different consoles. Authorization happens based on the JWT claims.

No.	Element	Key Consideration
2.	**Confidentiality and Integrity**	All applications should ensure "confidentiality" and "integrity" whenever required by adhering to transport and message-level security standards. (i.e., HTTPS, WS-Security)
3.	**Non-repudiation**	All applications should ensure non-repudiation by having standard audit-trails and provisions to have digital signatures.
4.	**OWASP Guidelines**	Open web application security project guidelines (OWASP) will be followed to protect from typical web attacks. The scope of testing will be limited to the most common web attack vectors, as identified by OWASP. (the top 10 OWASP was removed from the document) Refer the latest top 10 OWASP. *Reference: https://owasp.org/www-project-top-ten/*
5.	**Encryption**	Transport-level encryption is mandated across system/environment boundaries; hence, HTTPS will be used for external communications. Confidential data will be encrypted where relevant, using encryption keys applicable to the context of the data (i.e., application-level, user-level, session-level).This should entails data at rest and data at motion. The encryption algorithm to be used will be the Advanced Encryption Standard (AES), also known as Rijndael, at its maximum strength of 256 bits, using Public Key Cryptography Standard #5 (PKCS #5) with Password-based Key Derivation Function #2 (PBKDF2). Media file encryption has been provided to support PCI DSS. No portion of the data should be proprietary or vendor-encrypted, and all data should be accessible (reading, writing, querying, etc.) through standard IT protocols without vendor intervention. The biometric data, if used, should be stored as raw images (compressed for transmission, as allowed by the standard) from which the proprietary templates of any algorithm can be generated. Having the biometric image data ensures that migration to a new vendor template is possible. *NOTE: encryption will render encrypted data fields non-searchable.*

<table>
<tr><th>No.</th><th>Element</th><th>Key Consideration</th></tr>
<tr><td>6.</td><td>Hashing</td><td>Passwords will not be stored in a recoverable format but will be ‘salted’ based on a randomized seed and hashed for storage so that not even administrators can view the raw password itself. All variables related to this process will be provisioned via the context of the data being secured (i.e., application-level, user-level, session-level).

The BCrypt or similar password encoding approach can be used for hashing, using the default 10 logarithmic rounds of processing to generate a strong hash. Based on the trade-off of performance vs. security, this can be increased, if necessary.</td></tr>
<tr><td>7.</td><td>Digital Certificates</td><td>Public Key Infrastructure (PKI) using digital certificates provided by a trusted Certification Authority (CA) can be used for non-repudiation. This mechanism may also be used to identify the Foundational ID platform to third parties when consuming external services.</td></tr>
<tr><td>8.</td><td>Auditing</td><td>The operations listed below will be audited as a means of tracing actions/manipulation of data within the Foundational ID platform:
<table>
<tr><th>No.</th><th>Operations</th><th>Audit Storage</th></tr>
<tr><td>1.</td><td>Data Capture & Maintenance</td><td>Diagnostics Database</td></tr>
<tr><td>2.</td><td>Creation of Entry or Item</td><td>Diagnostics Database</td></tr>
<tr><td>3.</td><td>Modification of an Item</td><td>Diagnostics Database</td></tr>
<tr><td>4.</td><td>Deletion of an Item</td><td>Diagnostics Database</td></tr>
<tr><td>5.</td><td>Control or Status Change</td><td>Diagnostics Database</td></tr>
<tr><td>6.</td><td>Process Execution</td><td>Diagnostics Database</td></tr>
<tr><td>7.</td><td>Data Synchronization</td><td>Diagnostics Database</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>No.</th><th>Element</th><th>Key Consideration</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>8.</td><td>Print (only selected items)</td><td>Diagnostics Database</td></tr>
<tr><td>9.</td><td>Retrieval</td><td>Diagnostics Database</td></tr>
<tr><td>10.</td><td>Monitoring</td><td>Logs and Diagnostics Database</td></tr>
</table>
The system will have mandatory logging for all the transactions and these logs should be permanently available. The integrity of the logs should be maintained at all times.
All audit trails should be based on the principal of. write one.
Data is inclusive of (but not exclusive to) the executing thread identifier, timestamp, client IP address, client user-agent, server (internal) IP address must be stored per audit entry, where relevant.
</td></tr>
<tr><td>11</td><td>Security Framework</td><td>The Foundational ID platform Security framework should cover:
i) Solutions to ensure that core information assets are secure
ii) Secure all interactions including the complete lifecycle of registration centres (fixed and mobile), partners & any third parties interacting with the Foundational ID platform. It should also include all human interactions
iii) Governance, Compliance and Risks of the Foundational ID platform
Kindly refer the note below for details.</td></tr>
</table>

Table 2.3 : Security Elements for SL-UDI

Note: The different aspects of security framework are as follows

No.	Element	Key Consideration
1.	**Design Information Security Architecture**	The MSI should conduct a detailed assessment of information security needs of Foundational ID platform and develop the information security architecture incorporating the required security features/products.

No.	Element	Key Consideration
2.	**Information Security Automation**	The MSI's Security Automation should cover the following activities/processes: i) Incident Management and response including automation of incident collection, qualification and dispatching to respective owners. ii) Audit, Verification and Compliance including automation of testing (with minimal intervention), vulnerability and syslog analysis, creation of service requests with appropriate teams and priorities, and monitoring of incidents. iii) Controlling access via single sign-on iv) Service request automation v) Any necessary reports vi) BCP-DR tests including switchover, drills, and data verification vii) Certificate Service Provider dedicated to SL-UDI should be implemented.
3.	**Periodic vulnerability assessments**	The MSI should carry out quarterly vulnerability assessments in agreement with ICTA or nominated agency and fix any issues found. In the event where ICTA carries out a vulnerability assessment those identified vulnerabilities should be fixed by the MSI.
4.	**Network security**	The MSI shall be responsible for managing access to the Foundational ID platform network, ensuring that; i) The network shall be used *ONLY* for valid operational purposes and that networks are not used for personal and/or private activities. ii) Access to network and network resources provided only for ICTA authorized parties and follow SL-UDI policies and guidelines, iii) The MSI shall conduct quarterly access reconciliation audit exercises to ensure the process is adhered to.
5.	**Secure Data and Media Handling**	Guaranteeing the security of confidential information over public networks between various government agencies for authentication via the Foundational ID platform will be the MSI's responsibility. Ensuring the backups are current, complete, consistent, secure, and recoverable. MSI will be responsible for backup, testing, shipping

No.	Element	Key Consideration
		of backup tapes, retrieval of backup tapes and data recovery from tapes. Note: The backup site for tapes will be within Colombo and exact location will be informed to the successful bidder.
6.	**Business Continuity and Disaster Recovery**	The MSI should carry out BCP/DR tests in agreement with ICTA.
7.	**Supporting Security and Security & Network Operations Canter**	The MSI should ensure that the Foundational ID platform caters to the Security Operations Centre and Network Operations Centre requirements of ICTA. The Foundational ID platform should be capable of publishing analytics necessary to meet SOC and NOC requirements.
8.	**Audit facilities**	Wherever applicable, an audit trail of all activities must be maintained. On service or operation being initiated, the system should log the event, creating a basic 'audit log entry.' It should not be possible for the operation to be executed without the log entry being made. The information recorded in the audit trail depends on the type of activity which takes place. Each service would be responsible for logging detailed information. The different types of operations are - Data Capture & Maintenance, Creation of an entry/item, Modification an item, Deletion, Control (or status change), Process execution, Data synchronization, Print (only selected item), Retrieval, Monitor Detail logging may be enabled or disabled for each type of operation, and/or for each business object. It should be possible to configure which attributes of a data item should be traced at the detail level. Tracing of some attributes may be considered mandatory, and they should not be turned off. The data logs shall be retained and available as per the data retention policy defined by ICTA for SL-UDI. The following should be considered during the implementation

No.	Element	Key Consideration
		i) Support collection of system logs, application logs across devices, applications, servers, virtual machines, and containers ii) Support filtering of log levels (critical, error, warning, information) during collection iii) Support centralized collection of logs iv) Should support customizable log formats v) Support log rotation and configurable log file sizes for rotation vi) No log data should be lost during rotation vii) Support archival of logs at the log management servers viii) Support multiple transports/protocols for moving logs from the source to the destination ix) Support one or more centralized log server in a highly available mode x) The log servers should be horizontally scalable xi) Should support correlation of data across log files and data sources xii) Support search across log files xiii) Log server should support indexing for fast searches xiv) Log server should support customizable analytics on log data xv) Support integration with the dashboard for displaying analytical data
9.	**Backup and contingency planning**	The main contingencies that should be considered and the training with regards to these shall be given to the relevant staff – (i) Equipment failure, (ii) Physical/Natural Disaster, (iii) Messaging or communication facilities, (iv) Changes in operations and policy, (v)

No.	Element	Key Consideration
		The sudden absence of key personnel, (vi) Breach in Security, (vii) Automatic backups should be taken daily, weekly, and monthly, and (viii) All the backup procedures and backups need to be tested regularly for restoration.(ix) Performing backup drills. The Foundational ID platform should support heterogeneous backup storage media. The software should also leverage deduplication technologies for optimal usage of storage capacity. For databases, target-based deduplication should be leveraged and for desktops, host-based deduplication should be leveraged to reduce the amount of data getting replicated over the network. The application should also support the Backup architecture and replication strategy approved by ICTA. The following should be considered, i) Backup of file System, databases ii) Support backup with compression iii) Support secure backup with encryption and user provided keys iv) Support integration with backup media libraries, software defined storage v) Support disk to backup media and disk to disk backups vi) Support scheduling with multiplexing multiple streams to manage the SLAs vii) Support offsite backup and recovery viii) Support SDK, scripting to automate backup/recovery operations ix) Scheduled recovery from backup media. x) Recovery from remote sites

Table 2.4 : Different aspects of security framework

The following table provides an overview of the security tools required for the Foundational ID platform, please *refer to Annexure-3* for the comprehensive list of security tools. The MSI shall enrich and complement the tools if found necessary.

Identity & Access Management (IAM)	IAM tool is used for user access provisioning and de-provisioning for the Foundational ID platform. It ensures that the right people have access to the right resources.
GRC	This Foundational ID platform is used for managing the Governance, Risk and Compliance (GRC) program across the Foundational ID platform. Services which must be enabled by GRC are: Vulnerability Management, Incident Management, Risk Management, Vendor Management, Audit Management, Business Continuity Management and Audit modules policies. Documentation related to the some of the policies will be released to the selected bidder.
Application Security and SDLC	The Foundational ID platform security should be built into the software development process by using tools, technology, and processes. The security solution should manage the Open Web Application Security Project (OWASP) top 10 vulnerabilities and risks in the applications. i) **Broken Access Control -** Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits. ii) **Cryptographic Failures -** The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise. iii) **Injection-** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition. iv) **Insecure Design-** with a focus on risks related to design flaws. It calls for more use of threat modeling, secure design patterns and principles, and reference architectures. v) **Security Misconfiguration -** applications were tested for some form of misconfiguration. With more shifts into highly configurable software, vi) **Vulnerable and Outdated Components** - This a known issue that we struggle to test and assess risk. It is the only

	category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores. vii) **Identification and Authentication Failures** includes CWEs that are more related to identification failures. viii) **Software and Data Integrity Failures** focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. ix) **Security Logging and Monitoring Failures** This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics. x) **Server-Side Request Forgery** - The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time. For the latest please refer: *Refer <https://owasp.org/www-project-top-ten/> for the latest list as published which should be considered.*

Table 2.5 : Overview of the security tools required

2.2. Availability/Reliability

The system should have the following features for the availability and reliability.

No.	Element	Key Consideration
1.	**Redundancy & Failover**	Redundancy is the fault-tolerance technique used to increase the availability of the Foundational ID platform where a secondary node takes over when the primary node fails. The redundancy and failover

No.	Element	Key Consideration
		method will be defined in the design phase based on service type and requirements. The system should be reliable, with high-quality performance and the downtime should adhere to the agreed SLA. All components including integrations (i.e., ABIS, COTS) should be performed as follows – (1) Highly available unless the web/mobile application is designed with expected downtime for activities such as database upgrades and backups. (2) Hence to have high availability, the applications must have low downtime and low recovery time.
2	**Backup & Recovery**	A backup policy should be defined and implemented to ensure data recoverability in the event of accidental data deletion, corrupted information, or system outage. All data should be backed up fully/incrementally/differentially on a regular basis with the backups stored offsite to assist Disaster recovery. The medium of storage should be identified by those in charge of the production environment. The backup frequency and the information which needs to be backed up could be decided as per the customer request.
3	**Failure Detection and Recovery**	This should be designed in a manner to attempt recovery where and when it is possible. And if recovery is impossible, to fail gracefully - by ensuring transaction semantics (typically via rollback), making the required diagnostics/audit entries, and performing clean-up activities like closing connections, etc. All requests to the servers in the Foundational ID platform should pass through a proxy web server, operating in failover mode. The enrolment related processes will operate in an Active-Passive configuration whereas the authentication related processes will operate in Active-Active configuration. – Not relevant Scalability include to fault tolerant.

Table 2.6 : Availability and Reliability

2.3.Accuracy/Correctness

The system should have the following features for the accuracy and Correctness.

No.	Element	Key Consideration
1.	**Transactions**	The correctness of data – in terms of ACID properties (Atomic, Consistent, Integrity, and Durability) - will be ensured by the use of a transaction framework built into the programming frameworks used. All write operations (Create, Update, Delete), barring those exempted by specific functional requirements, should exhibit serializable behaviour; read operations, where relevant (e.g., for generating list views) may use a lower level of serializability, such as Read Committed.
2.	**Concurrency**	To maximize throughput, an optimistic concurrency model should be utilized, except where functional requirements dictate a pessimistic model, such as locking. The system should be designed to support the microservice architecture with an eventually consistent method. Concurrency is handled by providing event-based communication and orchestration of services based on events. Based on specific functional requirements, a higher granularity of concurrency checking (even up to field level) should be supported, though with an impact on performance and maintainability.

Table 2.7 : Accuracy/Correctness

2.4. Other Aspects

No.	Element	Key Consideration
1.	**Data Archival**	It is recommended that data archival be carried out frequently; the removal of transactional entities that are no longer valid/relevant will enable the Foundational ID platform to operate at maximum efficiency.
2	**Usability**	The application should be extremely usable; even a greenhorn user should be able to handle the system and incorporate all the functionality of the system in a simple and user-friendly interface as per the user's requirement. The application should be localized where necessary. The application should be responsive, where it should be viewable on any computing device. One of the main focus of the solution design will be to enhance the productivity of the end-users by following User Experience best practices. This will range from workflow design (minimizing the time

No.	Element	Key Consideration
		taken to complete a task) to the design of screens (which will make using the application a pleasant experience). Single Page Application (SPA) – technique needs used to design the user interfaces of the Foundational ID platform. This is a modern technique used by companies like Google in their Gmail offering, for immersive user experience. This will result in screens that load quickly without reloading the entire page, thereby providing the user with a better experience. The User Interface shall also be responsive, for a better viewing experience of mobile web browsers.
3	**Interoperability**	Publicly accessible applications should support the latest versions of the following browsers - Mozilla Firefox, Google Chrome, Apple Safari, Microsoft Edge Other applications interfaces (i.e., internal applications) should support the latest versions of the following browsers - Mozilla Firefox, Google Chrome, Apple Safari
4	**Robustness**	The application should be able to handle error conditions gracefully without failure. This includes tolerance of invalid data, software defects, and unexpected operating conditions. • **Failure Detection:** Once deployed, there should be appropriate tools to discover anomalies and failures of the system • **Fault Tolerance:** Application developers should anticipate exceptional conditions and develop the system to cope with them. The application must be able to use reversion to fall back to a safe mode, meaning, the application should continue its intended functions, possibly at a reduced level, rather than failing completely.
5	**Compliance with standards**	The code of application should be standardized by following web/mobile standards like W3C and ECMA – European Computer Manufacturers Association, to save time, augment the extensibility of the code, increase web/mobile traffic, and improve the accessibility and load time of the application.
6	**Reusability**	The application should use existing assets in some form with the software product development process. Assets are products and by-products of the software development life cycle and include code, software components, test suites, design, and documentation.

No.	Element	Key Consideration
		Standard coding practices and code documentation will be maintained in order to build quality reusable software and achieve the most gain from reuse. It is recommended that reuse takes place via the consumption of the service layer. As necessary, the functionality of the Foundational ID platform can be reused at the binary level.
7	**Multi-Lingual Support**	The application should be able to be accessed in Sinhalese, Tamil, and English. The user should be able to view applications in a usable manner in all three languages in any computing device.
8	**Scalability**	Suggested applications should be both scalable and resilient. A well-designed application should be able to scale seamlessly as demand increases and decreases. It should be resilient enough to withstand the loss of one or more hardware resources. The design of the Foundational ID platform will support both vertical and horizontal scaling, with vertical scaling (also known as 'scaling up') being the addition of more resources to existing deployment units (e.g., increasing processor power of existing servers). Horizontal scaling ('scaling out') being the addition expanded by adding processing, main memory, storage, or network interfaces to a node to satisfy more requests per system. The Foundational ID platform should be initially deployed in a scaled-out (clustered) configuration, with the minimal required deployment units. While vertical scaling can be used as a short-term measure to handle the increasing load, it is recommended that the more sustainable measure of horizontal scaling be moved to as quickly as possible.
9	**Portability**	Generalized abstraction between the application logic and system interfaces will be built for the usability of the Foundational ID platform in different environments.
10	**Legal and Licensing**	The application should comply with the national law of Sri Lanka.
11	**Configurability**	The Foundational ID platform should be made configurable where possible, to enable modification of system behaviour, post-deployment. This will be managed carefully (i.e., implemented only where required) to minimize any impact on the performance of the system. All the services build to comply with the 12-factor app

No.	Element	Key Consideration
		development framework, so the configurability is inbuilt with the system.
12	**Maintainability and Extensibility**	The code of an application should be properly documented with appropriate comments and no complex codes (highly cohesive and loosely coupled) to do modifications such as corrections, improvements, or adaption. The application should be designed and developed in a way that it can cater to future business needs. The attributes will be enhanced by the use of techniques such as Dependency Injection. System build assets of rest APIs and Integrations points are added to most of the high-level applications. API has been documented using swagger to support maintainability. From an engineering practice perspective, static analysis tools need be used to ensure maintainable code is being developed, while regular code reviews will further ensure the quality of the source code.
13	**Testability**	The application should be designed and developed in a way that testability is high, meaning, the ease of testing a piece of code or functionality, or a provision added in software so that test plans and scripts can be systematically executed. In simple terms, the software should be tested easily with the most famous five testing categories - Unit test, Integration test, System test, Safety test, and Experience test. Refer to Aden's (2016) view on semantic testing for more information. The MSI should ensure that the test coverage exceeds 90% with each release. The Test-driven development (TDD) approach should be used for unit tests to ensure minimal efforts on the implementation and facilitate correctness. Inversion of control (IoC) need be used to assist the development of such tests. Code coverage must be maintained at 95% or higher to achieve a higher degree of testability. A performance test will be performed to determine system parameters in terms of responsiveness and stability under various workloads. The test will provide an approximation of how many transactions per second can be supported. The scalability, reliability, and resource usage of the Foundational ID platform will be measured during the test. This process is expected to ensure that expected service levels are met in production by optimizing indicators such as network response time,

No.	Element	Key Consideration
		server query processing time, CPU memory consumption, etc. The MSI should ensure that the performance tests are fully automated and should be executable at any designated time with minimal manual intervention. Furthermore, schedule constraints allowing functional browser-based automated tests will be developed to test user interaction points. The web application should be working according to the given criteria in the latest version and five versions before in web browsers such as Mozilla Firefox, Google Chrome, Opera, and Apple Safari and the latest version and two versions before in Internet Explorer / Edge.
	Documentation	Provide the list of documentation and artifacts that needs to be submitted among others, product specifications, user guides and other training materials.

Table 2.8 : Other Aspects

2.5. Controls and Governance

The following mechanism should be implemented but not limited to.

No.	Element	Key Consideration
1.	**Operational Governance**	These involve internal policies and procedures for the operation. Further should align with the ISO/IEC 38500:2015. • Information security policies • Privacy policy and notices • Human resources policies • IT governance policy • Business continuity management and disaster recovery • Data retention policies • Communication to and acknowledgment by employees of policies

No.	Element	Key Consideration
2.	**Human Resources**	Screening of all employees, contractors, and consultants of MSI before their involvement in the implementation. This may include background checks, criminal history checks, and previous employment and credit checks. In some cases, a formal security clearance may be required for specific sensitive roles.
3.	**Supplier Vetting for COTS**	Due diligence for suppliers (i.e., System integrator) as well as periodic review of performance. This is to ensure that they can actually deliver on contractual commitments and that they have the qualifications and skills necessary for the quality of implementation.
4.	**Change Management**	Procedures to facilitate the adoption of change within the Foundational ID platform. Change control procedures should be designed to ensure that changes are appropriately considered, approved by management, and are not disruptive to the operations. Best practice standards are available, such as latest ISO/IEC 20000-1 Information Technology Service Management.
5.	**Audit and Compliance**	MSI is expected to carry out rigorous audits for the entire system, which would be conducted on a regular basis both internally and by trusted independent entities. The goal is to demonstrate the compliance of the UDI system with applicable laws and regulations, as well as internal policies, and that it operates effectively as designed and presented to the public.
6.	**Awareness**	Internal training and awareness for employees (i.e., DRP) to ensure they understand their roles and responsibilities in terms of overall solution, security and privacy, all other internal policies, etc.
7.	**Security and Privacy**	The MSI is required to comply to the below among others. i) Role-based system and logical access control to prevent system abuse. ii) Segregation of operational authority to combat malfeasance. iii) Secure audit logs to enhance investigative power in case of an incident and to provide deterrence. iv) Privacy controls.
8.	**Software License Guidelines**	i) Licenses for the required COTS software components must be drawn on behalf of ICTA. The licenses should be perpetual licenses including maintenance, upgrades, and support during the contracted period.

No.	Element	Key Consideration
		ii) Subscription licenses must cover the entire duration as mentioned in the RFP, and ICTA should have the right to renewal at expiry. iii) Software licenses must not be geographically restricted and the ICTA should be able to use the licenses at any time or place based on the needs of the project.

Table 2.9 : Controls and Governance

2.6. Interfaces, Monitoring, Incident Management and Helpdesk

2.6.1. Interfaces (APIs)

No.	Element	Key Consideration
1.	**API Management**	The services layer of the Foundational ID platform will function as an endpoint for integration consumers, by default, as a RESTful Application Programming Interface (API), using the JSON data format.
2	**API Standards and Best Practices**	API standards and best practices that *should be adhered* by the code. As specified by the link below. Refer: [https://github.com/microsoft/api-guidelines/blob/vNext/Guidelines.md]
3	**API Documentation**	In a service creation environment for developers, Swagger documentation should be provided.
4	**API Security**	The web/mobile application should use the appropriate API security protocol mentioned below. i) OAuth2 ii) No need to use cryptographic algorithms to create, generate, and validate signatures as all the encryption handled by TLS. iii) Recommend for less sensitive data applications iv) JWT (JSON Web/mobile Tokens)

No.	Element	Key Consideration
		v) Practice the principle of least privilege

Table 2.10 : Interfaces (APIs)

2.6.2. Monitoring/Instrumentation

Monitoring should be implemented at all levels of the application and its infrastructure. Dashboards and alerts should be implemented as required to monitor system health and availability in production. The Foundational ID platform monitoring should not cause any degradation in performance of the application. The following should be considered during the implementation not limited to:

i) Support non-intrusive monitoring of applications
ii) Support monitoring of response times of important transactions
iii) For Java Virtual Machine (JVM), monitor heap usage and Garbage Collection (GC) time
iv) Provide visual call graphs of key transactions along with execution time of all sub transactions
v) Provide transaction correlation across multiple application instances and across multiple applications (on the same or different physical/logical machines) in the call chain
vi) Provide option to enable/disable application monitoring during run time without restarting the applications
vii) Support monitoring of only selective sessions for a given set of service/function calls
viii) Support concurrent tracking of transaction response times of multiple applications or application instances
ix) The run time libraries required for the Foundational ID platform should be integrated with the DevOps process
x) Provide a visual dashboard to display call graphs of multiple applications/instances
xi) Allow multiple users to track and analyse their applications concurrently in the dashboard
xii) Provide role-based access to applications
xiii) Prepare Root Cause Analysis Reports for all critical incidents.
xiv) Monitor and Track all SLAs.
xv) Coordinate with OEMs (i.e. COTS) for resolving issues.

Database monitoring should have following capabilities,

The following should be considered during the implementation not limited to:

i) Monitor and audit all database activities independently including SELECT transactions and privileged users' activities, without any performance impact.
ii) Provide customizable policy definitions.
iii) Securely store the database activity logs/data outside the monitored database/data store preferably in a secure, reliable isolated data store.
iv) Generate alerts/notifications whenever policy violations are detected, integrate with SOC and the incident management system.
v) Aggregate and correlate database activities from multiple heterogeneous database management systems.
vi) Enforce separation of duties of database administrators, monitor the administrators' activities and prevent the manipulation or tampering of recorded activities or logs

2.6.3. Incident Management (Trouble Ticketing)

i) User Interface to log tickets and complete the process.
ii) Customizable workflow for the incident management process with escalation mechanism (escalation hierarchy) and approval processes.
iii) Define SLA for resolving tickets and support auto escalation of the tickets based on priority and SLA
iv) Support integration with other tools for auto generation of tickets and either automated or manual resolution of tickets.
v) Provide role-based access.
vi) Support multi-vendor workflow.
vii) Support integration with email, SMS.
viii) Integrated with SLA management tool for real time monitoring of tickets and SLA adherence / violations.

2.6.4. Technical Help Desk

i) User Interface to log technical help desk requests.
ii) Customizable workflow for the technical helpdesk request process with escalation mechanism (escalation hierarchy) and approval processes.
iii) Define SLA for resolving technical helpdesk request and support auto escalation of the requests based on priority.

iv) Support integration with other Enterprise Management System (EMS) tools for auto generation of technical helpdesk request and either automated or manual resolution of technical helpdesk request.

v) Provide role-based access.

vi) Support multi-vendor workflow.

vii) Support integration with email, SMS.

viii) Integrated with SLA management tool for real time monitoring of technical helpdesk requests.

ix) Log incidents/issues as service requests and provide a unique service request number. Acknowledgement should be sent to the user along with service ticket number through an email immediately on issue logging. All issues logged should be assigned a severity level (L1/L2 or L3). Indicative severity level definitions shall be discussed and finalized in consultation with ICTA.

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

xi) The Technical Helpdesk staff should have a provision to increase the severity levels, if required

xii) The Helpdesk staff shall have provisions through the application for coordinating with concerned vendor in case issues are pertaining to any external entity product/support

xiii) The MSI shall analyse all the incidents and provide a root cause analysis report on a periodic basis for all the recurring incidents. MSI shall ensure that resolution is provided for these problems by respective technical teams/vendors to prevent further issues due to the same cause. The report for the same should be submitted to ICTA.

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

xv) Issues which cannot be resolved by the Technical Helpdesk should be routed to the concerned team of the MSI for resolution.

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

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

xviii) Each service request would have a unique service request number.

xix) It is the responsibility of the MSI to ensure quality of the Technical Helpdesk.

xx) All incidents should be recorded. These records shall be retained on disk for easy retrieval.

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

xxii) The Technical Helpdesk should comply with SLAs applicable to them.

xxiii) Continuous Improvement: The MSI shall ensure continuous improvement in the Technical Helpdesk Operations.

xxiv) The MSI shall prepare and submit reports to ICTA as per the mutually agreed reporting structure.

2.6.5. Reporting

i) Provide Customizable Reports

ii) Provide PDF, CVS report formats

iii) Provide Real-time Dashboard for reports

iv) Reports Classification by SLA, Priority, Incident Type, Application, Vendor etc.

v) Ability to create templates by reporting administrator for creation of new reports

vi) Ability of scheduled reporting

vii) Reports to be integrated with respective modules as well as integrated reporting module