



**THE GOVERNMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF
SRI LANKA**

Ministry of Telecommunication and Digital Infrastructure

BIDDING DOCUMENT – SECTION VI – SCHEDULE OF REQUIREMENT

Volume 2 of 3

Single Stage Two Envelopes Bidding Procedure

FOR THE

PROCUREMENT OF DESIGNING, DEVELOPING, SUPPLYING, DELIVERING,
INSTALLATION AND IMPLEMENTING THE SOFTWARE, HARDWARE AND
INFRASTRUCTURE FOR GENERATING DIGITAL IDENTITY FOR CITIZENS OF
SRI LANKA AND FOR THE HOUSEHOLD TRANSFER MANAGEMENT (HTM) SYSTEM

INVITATION FOR BIDS No: MTDI/GOSL/IS/ICB/2016/15

April, 2016

Abbreviations

Please note the following abbreviations used throughout this tender document.

API	Application program Interface
BOM	Bill of Material
BOT	Build Operate Transfer
DTC	Digital Transaction Card
DS	Divisional Secretariats
DIP	Digital Instruction Providers
HTM	Household Transfer Management
NDF Centers	National Digital Facilitation Centers (both District and DS centers)
NDI	National Digital Identity
NDI Platform	National Digital Identity Platform
NSC	National Steering Committee
KB	Knowledge Base
LGC	Lanka Government Cloud (G- Cloud)
LGN	Lanka Government Network (G- Connect)
OAT	Operational Acceptance
PoC	Proof of Concept
POM	Project Operational Manual
SLA	Service Level Agreement
UAT	User Acceptance Certificate

Table of Contents

1.	The Employer	6
2.	Vision of a digitally inclusive society in Sri Lanka.....	6
3.	Proposed Concept of the Household Transfer Management (HTM) System.....	10
3.1	Introduction	10
3.2	Current Situation and Key problems.....	10
3.3	Objective of the HTM project.....	11
3.4	Proposed implementation approach	12
3.5	Overall Implementation Approach.....	12
4.	The Scope of Services.....	17
4.1.	General	17
4.2.	[Item 1] – Enrolment Stations	23
4.3.	[Item 2] – Portable Units.....	24
4.4.	[Item 3] - Centralized NDI Software Solution	25
4.5	[Item 4] - Training of Enrollment Staff.....	34
4.6	[Item 5] - Digital Transaction Cards (DTC) and Personalization	37
4.7	[Item 6] - NDI Hosting Infrastructure.....	44
4.8	[Item 7] - NDI Certification Service Provider (Certification Authority) and Services.....	47
4.9	[Item 8] - Household Transfer Management (HTM) system	48
4.10	Review Committees and Review Procedures.....	52
5	Warranty and Service Level Agreement (SLA)	53
5.1	[Item 1] - Enrolment Stations.....	53
5.2	[Item 2] – Portable Units.....	56
5.3	[Item 3] – Centralized NDI Software Solution	59
5.4	[Item 5] – Digital Transactions Card (DTC) and Personalization	62
5.5	[Item 6 and 7] – NDI Hosting Infrastructure and Certificate Authority	63
5.6	[Item 8] – Household Transfer Management (HTM) System.....	66
5.7	General	69
6	Bill of Material (BOM)	70
7	Specifications	72
7.1	[Item 1] - Enrolment Stations.....	72
7.2	[Item 2] - Portable Unit	79
7.3	[Item 3] - Centralized NDI Software Solution	80
7.4	[Item 4] – Training Enrolment Staff	84
7.5	[Item 5] - Digital Transaction Cards and Personalization.....	85
7.6	[Item 6] - NDI hosting infrastructure	96
7.7	[Item 7] - NDI Certification Service Provider (Certification Authority) and Services.....	100
7.8	[Item 8] – Household Transfer Management (HTM) system	101

8	Facilities and services provided by the Employer	103
8.1	Key Activities.....	103
8.2	NDF Centers (Proposed).....	104
8.3	Training of enrolment staff	107
8.4	Digital Transaction Cards (DTC) and Personalization	107
8.5	NDI Hosting Infrastructure	107
9	Locations	108
10	Implementation Schedule	114
11	General Requirements	115

INSPECTION COPY

Table of Figures

- Figure 1: National Digital Identity and Transaction Framework
- Figure 2: Project Duration
- Figure 3: Household Transfer Management System
- Figure 4: NDI core and NDT platform
- Figure 5: Major components (Hardware layer) of NDI
- Figure 6: Card Personalization process
- Figure 7: Proposed structure for the production site
- Figure 8: Production Data Center I & II
- Figure 9: Schematic for NDI Certificate Authority
- Figure 10: High-level conceptual view of the household transfer management (HTM) system
- Figure 11: High level architecture of the Household Transfer Module implementation
- Figure 12: Proposed enrolment station / desk
- Figure 13: Proposed Manager /Supervisor station / desk
- Figure 14: Layout between stations / desks
- Figure 15: Proposed DS NDI center layout
- Figure 16: Proposed District NDF center layout.

**PROCUREMENT OF DESIGNING, DEVELOPING, SUPPLYING,
DELIVERING, INSTALLATION AND IMPLEMENTING THE SOFTWARE,
HARDWARE AND INFRASTRUCTURE FOR GENERATING DIGITAL
IDENTITY FOR CITIZENS OF SRI LANKA AND FOR THE HOUSEHOLD
TRANSFER MANAGEMENT (HTM) SYSTEM**

1. The Employer

The Ministry of Telecommunication and Digital Infrastructure (MTDI), Sri Lanka, is the policy making body of the country related to the subject of telecommunication, IT and digital technologies.

Accordingly, the Vision of the Ministry is transforming Sri Lanka to "*a digitally empowered nation*".

To materialize the above vision, the following strategies have been deployed, considering medium- and long-term objectives of the country, especially the agenda for "digitizing the economy".

- Improve the digital infrastructure of Sri Lanka for facilitating the enhancement of digital ecosystems
- Utilize the ICT for improving the governance
- Enhance the ICT policies, legislations and standards
- Improve the use of ICT applications in key sectors
- Improve citizens' engagement/participation in ICT enabled society
- Facilitation of ICT industry development
- Facilitate trade and business sectors through ICT

The Information and Communication Technology Agency (ICTA) of Sri Lanka is the responsible for the implementation of the proposed HTM Solution.

ICTA is the apex ICT institution of the Government. In terms of the Information and Communication Technology Act No. 27 of 2003, (ICT Act) ICTA has been mandated to take all necessary measures to implement the Government's Policy and Action Plan in relation to ICT. In terms of Section 6 of the ICT Act, ICTA is required to assist the Cabinet of Ministers in the formulation of the National Policy on ICT and provide all information necessary for its formulation. ICTA, which is wholly owned by the Government of Sri Lanka, implemented the e-Sri Lanka Development Project under which significant progress has been made.

2. Vision of a digitally inclusive society in Sri Lanka

The adoption and usage of online services, including e-Commerce activities by citizens are at an increasing rate; with all statistics indicating an exponential growth in this segment of online users. Even by now the above segment of citizens are going

online for obtaining various services. This includes, among others, online shopping, e-Channeling for doctor appointments, banking, online transactions and obtaining government services.

Despite the above growth, there is a question as to why the citizens currently cannot rely on online systems for obtaining all services.

For example citizens currently cannot perform actions such as signing contracts online, apply for a passport, voting from home, make payments to all commercial transactions - including high value payments such as custom duty; access to personal documents online, access to medical records online, access car insurance history.

There are private schools which allows parents to pay the term fees online; yet for administrative matters, parents are required to sign a physical document indicating liability waiver, if the their children are enrolling to certain sports such as hockey, boxing.

All the above has been attributed to one key reason that there is no mechanism for the existing software systems /online services to identify the users/ citizens with enough confidence to provide the services that they expect.

Despite the perceived digital transformation over the years, the method of proving the identity of the users / citizens has remained locked in a traditional physical mode, with paper or plastic documents.

Therefore, the reliance on traditional modes of proving identification and authentication is becoming a significant barrier for offering online services and for facilitating technology innovation.

The government of Sri Lanka has a vision to achieve a digitally inclusive society in Sri Lanka by bringing about digital commerce to facilitate governments, businesses and citizens to be able to perform digital commerce and financial transactions with efficiency, ease and at a reduced cost.

To achieve the above, the government intends establishing a National Digital Identity (NDI) through a National Digital Transaction (NDT) platform. This vision has been endorsed by Parliament of Sri Lanka, as The Budget Proposals of 2016 pledged such a system for the citizens. Accordingly, the NDI initiative intends to establish a digital identity to every citizen in the country, enabling them to perform, among others, digital financial transactions leveraging on the NDT platform.

The proposed NDT platform is a secure national middleware infrastructure that will facilitate the following digital interactions and digital commerce in the country;

- 2.1. Digital interactions by citizens with government institutions, as well as with private sector, in order to utilize services such as passport applications, submitting of tax returns, and for obtaining any sensitive information /services and to issue secure instructions.

- 2.2. Digital commerce and ease of performing secure digital transactions for government, businesses and citizens. This includes digital transactions between government organizations (G2G), Government to business (G2B), Government to Citizens (G2C), Businesses to Businesses (B2B), Businesses to Citizens (B2C) and transactions between citizens (C2C).

This project will also facilitate the implementation of a fully integrated and an automated system to manage household transfers, including rationalization of costs for the absolutely needy who are associated with all Welfare and SafetyNet programs including Pensions as has been identified by the Ministry of Finance as the key project resulting from the implementation of the above NDI and NDT Platforms.

Though this project is intended to cover beneficiaries associated with the above mentioned pension, social welfare and safetyNet programs, subsequently, any citizen, even if they are not registered as beneficiaries, but receiving related services such as free treatment from government hospitals, could also be included. This will go a long way to achieve the government's vision of a digital society.

Refer below Figure 1 for the above mentioned NDI & NDT Framework, which was tabled during the budget speech of 2016.

National Digital Identity & Transaction Framework

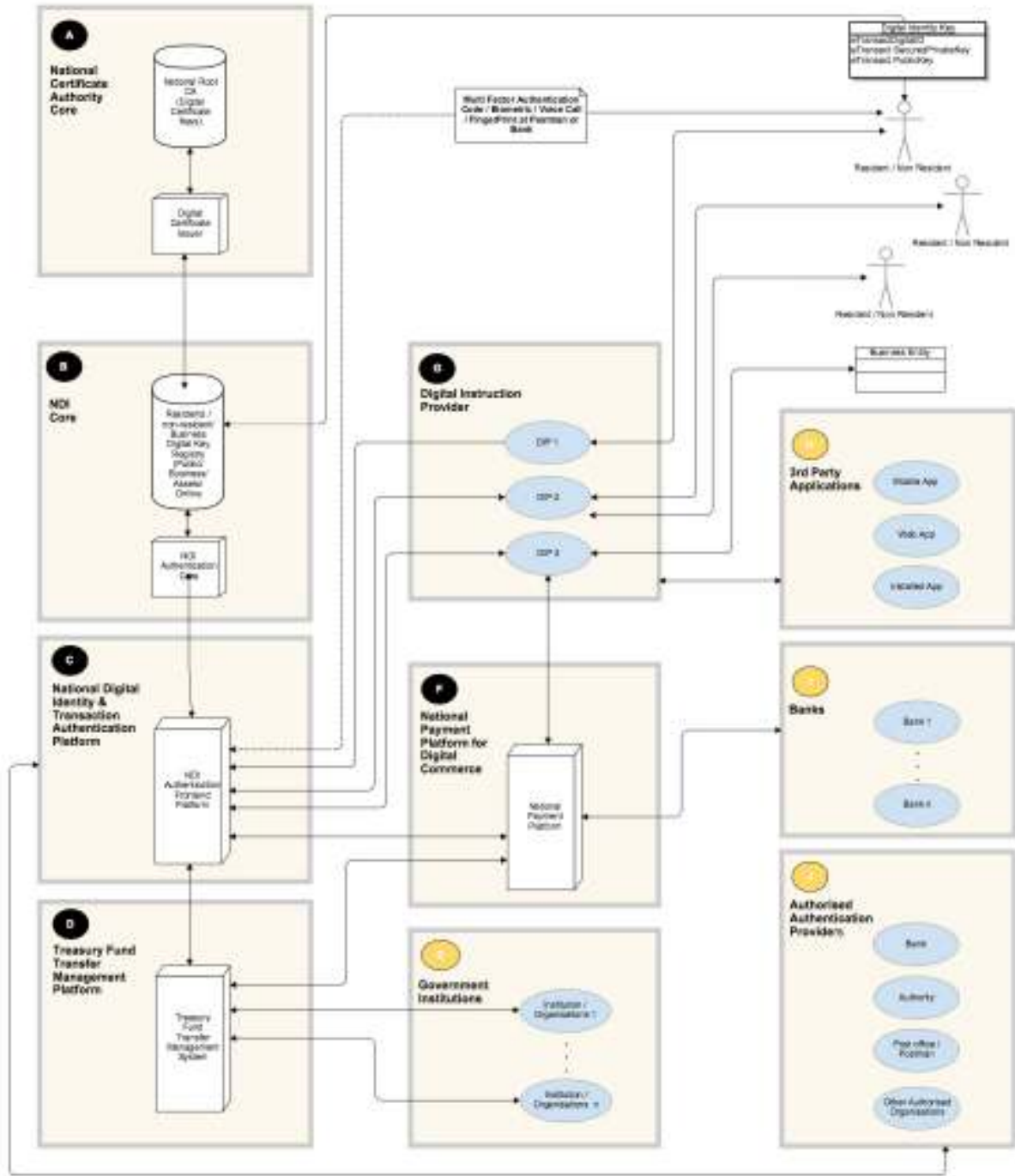


Figure 1: National Digital Identity and Transaction Framework

3. Proposed Concept of the Household Transfer Management (HTM) System

3.1 Introduction

The Government of Sri Lanka annually allocates funds for the social welfare, safety net programmes and pensions. These programs are designed to protect citizens from the economic risks and insecurities of life. The most common type of programs provide benefits to the elderly or retired, the sick or invalid, dependent survivors, mothers, the unemployed, the work-injured, school children and families. It is estimated that at present, approximately 249 billion rupees are spent by the government annually for these social welfare, safety net programmes and pensions.

At present, there is no centralized solution in place to monitor and manage these welfare programmes. As a result the Government has no way of ensuring among others, that the subsidies are distributed to the right beneficiaries, adequate measures are to be taken to reduce unnecessary costs and duplications, and eliminate misuse.

In view of the above, the Cabinet of Ministers granted approval to the Cabinet paper no 15/1303/719/017, a Memorandum dated 2015-09-22 by the Minister of Finance on implementing a fully integrated and an automated system to manage all Welfare and Safety Net Programmes in Sri Lanka, in order to ensure the effective use of household transfers and to include rationalization of costs for the absolutely needy. The Cabinet of Ministers granted approval for the following;

1. To establish a ‘Centralized Household Transfer System’ for the social safety net programmes in the country.
2. To Instruct to the Information and Communication Technology Agency of Sri Lanka (ICTA), being the apex ICT institution of the Government under the ICTA Act of 2003;
 - a. To formulate a centralized solution to fulfill the key objectives of the Government for the efficient management of the Household Transfer System;
 - b. To obtain the required assistance for the purpose from the relevant government institutions and all other stakeholders, with a view to issuing a ‘National Digital Unique Identifier (Social Security)’

3.2 Current Situation and Key problems

- 3.2.1 As elaborated above, one of the main concerns of the government with regard to Pensions, Welfare and Safety Net programs, is the that there is a significant number of duplications among multiple beneficiary programmes where the exact number of beneficiaries cannot be ascertained due to the lack of an efficient and accurate monitoring system. As a result government funds may be wasted or misused.

- 3.2.2 One of the key concepts that the proposed project intends to address, is the issuance of a ‘National Digital Unique Identifier (Social Security)’. Currently there is no mechanism for identifying / authenticating an individual uniquely during digital interactions. As a result, most of the financial and important transactions are carried out manually, despite having cross-government solutions.
- 3.2.3 Shall there be such a unique identifier, all government and private sector systems will be able to recognize each individual interacting with systems, and would be able to communicate and transact securely. Currently there is much inefficiency in citizens interact with others and with institutions as a result of not having such a unique identifier.
- 3.2.4 Many government organizations are planning to issue their own digital transaction cards. Further none of those cards carry a digital identifier. Such multiple projects are a waste of government funds. However if the government decides to issue a single digital card, incorporating among others, a unique digital identifier of the owner; then it may have a wide verity of use.
- 3.2.5 Further there is no such government initiative intending to issue digital identifiers to citizens. This fact emphasis the timely need for rapidly executing the proposed HTM project, intended for all beneficiaries and further extended to al citizens with necessary approvals.

3.3 Objective of the HTM project

Therefore with the proposed HTM solution the government intends to address the current concerns with regard to proper management of government funds associated with social welfare programs and pensions, and in the process, facilitate the implementation of national digital infrastructure which will enable the government to initiate several other key initiatives.

The unique digital identifier is generated leveraging biometrics of each individual. Though there are number of instruments such as the SIM, Tokens, Smart Cards and Phones which can be used to store this, it has been identified that the Smart Cards to be a comparatively the low cost, durable solution and that can be issued to citizens. The beneficiaries can make use of this smart card as to multi-factor authentication and for performing digital commerce. With the government National ICT policy, there shall be number of such online services delivered via multiple channels to citizens including the rural community.

Following are the key objectives intended to be achieved by the Ministry of Finance of the proposed HTM project;

- a. Justify spending of the government for Pensions, Welfare and Safety Net programs by ascertaining the accurate number of beneficiaries.
- b. Facilitating stakeholder organizations associated with beneficiary programs for efficiently managing respective social welfare, Safety net programs and pensions through central monitoring and management system.
- c. Efficiently facilitating a mechanism which will enable the government to offer more benefits to ‘absolute needy’ by lowering the administrative costs.

3.4 Proposed implementation approach

3.4.1 Key Activities

Following has been identified as key activities in order for implementing the proposed solution.

- 3.4.1.1 Ensuring the legal mandate for implementing HTM project
- 3.4.1.2 Identifying the beneficiary population
- 3.4.1.3 Develop an ICT solution for data capturing and storing.
- 3.4.1.4 Collection of information including biometrics from beneficiaries
- 3.4.1.5 Generate unique digital identifier to beneficiaries
- 3.4.1.6 Implement a national authentication platform for real-time authenticating request made by stakeholder organizations.
- 3.4.1.7 National middleware infrastructure facilitating cross-government secure data communication.
- 3.4.1.8 Integrated transaction platform for facilitating direct transfer of funds to beneficiary accounts.
- 3.4.1.9 Personalization and issuance of a Digital Transactions Card to all beneficiaries.
- 3.4.1.10 Development of Treasury Management System for facilitating issuance of digital instructions to transfer funds directly to the actual beneficiaries.
- 3.4.1.11 Improvements to the systems at stakeholder organizations associated with beneficiary programs

3.5 Overall Implementation Approach

Seq.	Activity	Implementation approach
3.5.1	Ensuring the legal mandate for implementing HTM solution	<ul style="list-style-type: none"> ▪ The employer will obtain the required legal mandate prior to commencing the implementation of the HTM solution.
3.5.2	National Steering Committee (NSC)	<ul style="list-style-type: none"> ▪ A national steering committee for the HTM project has been established to achieve the

		<p>following objectives;</p> <ol style="list-style-type: none"> 1 To ensure participation of all stakeholder organizations associated with the pensions, social welfare and safetyNet programs. 2 To ensure successful integration to the National Digital Identity (NDI) and National Digital Transaction platforms by stakeholder organizations.
3.5.3	Identifying the beneficiary population	<ul style="list-style-type: none"> ▪ The total population is determined as approximately 20 million in accordance with the Population and Housing, Census conducted by the Department of Census and Statistics. ▪ Considering the practical concerns with related to the HTM objectives, the initial target beneficiary population has been decided as 14 million citizens by the National Steering Committee of this project. ▪ Beneficiaries are located throughout the country.
3.5.4	Develop a centralized NDI solution (With this contract)	<ul style="list-style-type: none"> ▪ The Employer will procure a service provider in order to develop a central NDI solution and related integrations. ▪ The central database shall have a key integration with the Population Registry, for real-time updates.
3.5.5	National policy on collection, storage, sharing and use of citizens' personal data	<ul style="list-style-type: none"> ▪ A committee has been setup for formulating a national policy on collection, storage, sharing and use of citizens' personal data. The Ministry of Telecommunications & Digital Infrastructure has taken action for setting up the committee, and by now the committee is actively working on prerequisite activities in order for formulating the policy.
3.5.6	Collection of information including biometrics from beneficiaries (With this contract)	<ul style="list-style-type: none"> ▪ The employer will procure a service provider in order for setting up the data collection centers, which are referred National Data Facilitating Centers (NDF). ▪ Enrollment centers shall be located across the country based on District and Divisional

		<p>Secretariat (DS) boundaries.</p> <ul style="list-style-type: none"> ▪ Aspects with regard to connectivity and secure communication for NDF centers shall be facilitated via Lanka Government Network (LGN). <p><u>Unique Digital Identity</u></p> <ul style="list-style-type: none"> ▪ Individual’s (beneficiaries) biometrics (i.e. Iris, finger print, and face) and unique identifiers; transformed /stored in digital form, which can be authenticated by software systems during digital interactions, in order to identify/ verify the person. ▪ The employer will procure the required biometric data capturing devices and other equipment. ▪ The employer will setup data verification and operations centers. ▪ As part of the National ICT strategy, above mentioned biometric data capturing devices and centers will be setup as part of cross-government digital Infrastructure, indented to be used by other government organizations for services delivery in future.
<p>3.5.7</p>	<p>Issuance of unique digital identifier to beneficiaries (With this contract)</p>	<ul style="list-style-type: none"> ▪ Biometrics (i.e. Iris, finger print, and face) collected from beneficiaries will be used for uniquely identifying the citizens before generating Public and a Private keys which will be issued to each citizen. ▪ These will be used for authentication by software systems during digital interactions, in order to identify/ verify a person. ▪ The NDI Certification Service Provider (NDI Certification Authority) will issue digital certificates for the verified citizens. National Certification Authority will certify the NDI Certification Service Provider based on the provisions given by the Electronic Transactions Act. ▪ NDI Certificate Authority will be established for issuing unique digital identifier for beneficiaries

3.5.8	Implement a national authentication platform for real-time authenticating request made by stakeholder organizations. (With this contract)	<ul style="list-style-type: none"> ▪ The employer will procure a service provider in order for formulating associated key components of the authentication platform which shall facilitate authentication requests made by stakeholder organizations. ▪ As part of the National ICT strategy, the proposed authentication platform will be setup as part of cross-government digital Infrastructure, indented to be used by other government organizations for services delivery. ▪ Aspects with regard to connectivity and secure communications shall be facilitated via Lanka Government Network (LGN).
3.5.9	National middleware infrastructure facilitating cross-government secure data communication. (Already implemented)	<ul style="list-style-type: none"> ▪ The Lanka Gate middleware infrastructure will facilitate this requirement. ▪ The LankaGate is part of the existing national common infrastructure implemented by ICTA for cross-government service delivery.
3.5.10	Integrated transaction platform for facilitating direct transfer of funds to beneficiary accounts. (Currently being implemented)	<ul style="list-style-type: none"> ▪ The National Payment Platform (NPP) which is integrated with financial institutions and LankaClear shall facilitate this requirement. ▪ NPP is part of the proposed National Digital Transaction (NDT) platform approved by the Hon Members of the Parliament (MPs) through the budget speech of 2016.
3.5.11	Personalization and issuance of a Digital Transactions Card (DTC) to all beneficiaries. (With this contract)	<ul style="list-style-type: none"> ▪ The DTC is the proposed instrument to be used given to beneficiaries, which stores their digital identity. ▪ The DTC shall facilitate secure communication and financial transactions initiated by the owner.
3.5.12	Software solution for the Ministry of Finance for facilitating issuance of digital instructions to transfer funds directly to the actual beneficiaries (With this contract)	<ul style="list-style-type: none"> ▪ The employer will procure a service provider for implementing a software solution.
3.5.13	Improvements to the systems at stakeholder organizations	<ul style="list-style-type: none"> ▪ The employer will procure service providers in order for integrating existing solutions or for

	associated with beneficiary programs	developing new solutions for beneficiary programs.
--	--------------------------------------	--

Table 1: Overall Implementation approach

INSPECTION COPY

4. The Scope of Services

Description	Bidders Compliance	Reference (Section No and Page NOs)
4.1. General		
<p>The bidder shall fulfill / facilitate all of the following;</p> <ul style="list-style-type: none"> 4.1.1. Understand the overall scope of the initiative. 4.1.2. Supply, Delivery, Installation and Commissioning of data collection equipment, computer hardware and furniture at enrolment Stations located at NDF centers. 4.1.3. Supply, Delivery, Installation and Commissioning of data collection portable equipment. 4.1.4. Setting up of a centralized software solution to capture, store, and update collected NDI data and authenticate during operations. 4.1.5. Training of staff associated with collection of data. 4.1.6. Supply, delivery, installation, commissioning, personalization and issuance of Digital Transaction Cards (DTC) and related equipment. 4.1.7. Supply, delivery, installation and commissioning of systems infrastructure to host the proposed centralized NDI software solution. 4.1.8. Supply, delivery, installation and commissioning of the Certification Service Provider (Certification Authority) and establishment of Signature Signing and Authenticating Services. 4.1.9. Development of a centralized software solution to transfer funds to respective citizens. 4.1.10. The employer will fulfill the facilities and services as indicated in “8. Facilities and services provided by the employer” of the document. The bidder work in collaboration with the employer in order to full fill the objectives of this project. 4.1.11. Further to above, any dependent actions / services should be mentioned by the bidder to the employer in advance and should finalize the implementation schedule collaboratively. 		

<p>4.1.12. Further to above, the bidder should carry out integrations such as connectively to LGN network</p> <p>4.1.13. The bidder shall formulate an “Operational Manual” outlining, among others, maintenance and operational aspects. The operational manual shall include all relevant sub-manuals that would outline procedures and relevant criterions which would facilitate all stakeholders associated with this project for successful operational governance</p> <p>4.1.14. This shall be one of the key documents for the User Acceptance Test (UAT). The UAT shall be conducted to give acceptance commence operations.</p> <p>4.1.15. A complete UAT document shall be supplied by the bidder including all positive and negative testing scenarios. The bidder shall also review and resubmit the UAT document including the comments and observations made by the employer.</p> <p>4.1.16. A complete Operational Acceptance Test (OAT) document shall be supplied by the bidder. The bidder shall also review and resubmit the OAT document including the comments and observations made by the employer.</p> <p>4.1.17. The Operational Acceptance Test (OAT) shall be conducted once the bidder completes successful commissioning of all items specified in this project.</p> <p>4.1.18. The UAT and OAT criterions shall be discussed agreed upon. The Employer has the final decision on the criterion, in accordance with the contract scope.</p> <p>4.1.19. The total project duration is as specified below;</p> <p>4.1.19.1. The total project duration is 5 years and 6 months from the contract effective date. This includes the following in accordance with the delivery schedule;</p> <p>4.1.19.2. Time duration up to the commencement of the UAT is 4 months.</p> <p>4.1.19.3. The UAT time period is 1 month</p> <p>4.1.19.4. Project operational time duration from the date of UAT acceptance is 5 years.</p> <p>4.1.19.5. However the bidder shall be able to commence the OAT acceptance within 12 months from the date of UAT acceptance.</p> <p>4.1.19.6. The OAT time period is 1 month</p> <p>4.1.19.7. Project operational time duration from the date of OAT acceptance is 4 years.</p>		
---	--	--

- 4.1.19.8. The contract end date shall be in accordance with the time duration specified in above points (4.1.16.1), (4.1.16.4) and (4.1.16.7).
- 4.1.19.9. Refer below Figure 2 for a graphical view of the project key milestones.

Key Milestones \ Months	Year 1												Year 2												Year 6							
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12					3	4	5	6
Project Implementation																																
UAT																																
Rollout - all NDF centers																																
OAT																																
Post OAT operational time																																

LAUNCH ->

Figure 2: Project duration

- 4.1.20. During the UAT / OAT period there shall not be any issues of severity levels 1 or 2 reported / identified. If so it is considered as a failure.
- 4.1.21. The bidder is required to adhere strictly to the warranty and service levels.
- 4.1.22. The bidder shall ensure 24x7 available helpdesk and issue reporting system. The helpdesk shall support three languages (English/ Sinhala and Tamil), and shall be efficient. The bidder shall provide an SLA for the operations of the helpdesk which shall complement the overall project SLAs.
- 4.1.23. The bidder shall be responsible for the successful and timely delivery of the project.
- 4.1.24. Project Director/Manager appointed by the bidder is responsible for the delivery of the project (single point of contact) shall liaise with the Employer and work closely with the employers project management team with regard to all matters related to the project.
- 4.1.25. Project Director/Manager appointed by the bidder is responsibilities include among others;
 - 4.1.25.1. Attending all project meetings
 - 4.1.25.2. Ensure relevant project team members participate project meetings
 - 4.1.25.3. Ensure all internal and external communications and escalations are done to avoid delivery delays.
 - 4.1.25.4. Delivery of the project successfully.
 - 4.1.25.5. Submit weekly progress reports to the relevant committees. I. e. project implementation committee.
 - 4.1.25.6. Ensure the help desk and related support functions are in place.

- 4.1.26. The bidder shall submit a detailed project proposal at the commencement of the project and shall obtain acceptance from employer. The project proposal should include all aspects up to the acceptance of the OAT.
- 4.1.27. The project proposal shall be improved based on the decisions made by the project steering committee (NSC).
- 4.1.28. The bidder shall be able to undertake maximum of 5-years post warranty support services. During this time period, the same warranty and SLAs for respective Items shall be applicable (What had been enforced / applicable during the 5-year services support period). The bidder shall provide pricing for the post warranty time period.
- 4.1.29. The bidder shall ensure a smooth and professional hand over of the related project components and artifacts at the end of the contractual time period.
- 4.1.30. Warranty and Service Levels are applicable from the date of UAT acceptance certificate is issues to the bidder.
- 4.1.31. The bidder shall submit the following reports to the employer. The bidder should elaborate in detail all reports to be submitted. If there are any sub-reports associated with the ones mentioned below; if so the bidder should specify. The bidder should also specify any reports which are not specified in below table.

Reports	Submitting time period / project milestone
1. Project proposal(s)	
2. System Requirement Specification(s)	
3. Detailed Technical design document(s)	
4. Quality Assurance Plan(s)	
5. Compliance document(s) – functional and non-functional requirement(s)	
6. User Manual(s)	
7. Training Plan and Training materials	
8. IS Audit reports and certifications	
9. UAT documents	
10. OAT documents	
11. Operational Manual(s)	
12. Procedure Manual(s)	

13. Project Management related document(s)

Table 2: Reports

4.1.32. NDF centers

The Employer will setup NDF data collection centers throughout the country. Following indicates the proposed number of centers and respective enrolment desks. This may vary depending on the site location and respective decisions taken by the NSC during the project implementation phase.

NDF Centers		No of Enrollment Desks	Number of Centers
District Centers	Type A	50	6
	Type B	40	6
	Type C	30	4
	Type D	10	13
Total No of NDF District Centers			29
Total No of NDF Centers at Divisional Secretariats (DSs)			331

Table 3: NDF centers

4.1.33. The Employer will to procure following project components via this contract

Project Components	Name	Item Description	Locations
Item 1	Enrolment Stations	Supply, Delivery, Installation and Commissioning of data collection equipment, computer hardware and furniture at enrolment Stations located at NDF centers.	29 + District Centers and 331+ DS s located throughout the country.
Item 2	Portable Units	Supply, Delivery, Installation and Commissioning of portable equipment for data collection.	Colombo HTM project Operations Center
Item 3	Centralized NDI Software Solution	Setting up of a centralized software solution to capture, store, and update collected NDI data and authenticate during operations.	NDI Hosting Infrastructure, Colombo

Item 4	Training	Training of staff associated with collection of data	At NDF Centers throughout the country OR suitable locations specified by the bidder.
Item 5	Digital Transaction Cards (DTCs) and personalization	Supply, delivery, installation, commissioning, personalization and issuance of Digital Transaction Cards (DTC) and related equipment.	29+ District Centers
Item 6	NDI Hosting Infrastructure	Supply, delivery, installation and commissioning of systems infrastructure to host the proposed centralized NDI software solution.	Colombo
Item 7	Certification Service Provider (Certification Authority) and services	Supply, delivery, installation and commissioning of the Certification Authority and establishment of Signature Signing and Authenticating Services	Colombo
Item 8	Household Transfer Management (HTM) system	Development of a centralized software solution (HTM system) for the Ministry of Finance, to transfer funds to respective citizens.	Colombo

Table 5: Project Components

4.1.34. After obtaining the UAT certificate, during the project 5-year operational period there could be enhancements that needs to be accommodated by the proposed solution. In view of the above, the bidder should undertake change requests amounting to 500 person-days of Development, Quality assurance and configurations to the proposed solution, with no additional cost to the employer.

Description	Bidders Compliance	Reference (Section No and Page NOs)
4.2. [Item 1] – Enrolment Stations		
<p>4.2.1. The NDI solution including the enrolment software shall facilitate the collection of the following biometric data.</p> <p>4.2.1.1 2D Facial Image (Photo)</p> <p>4.2.1.2 Finger prints (10)</p> <p>4.2.1.3 Iris scan</p> <p>4.2.2. The NDI solution including the enrolment software shall facilitate the collection of the following scanned images, among others,</p> <p>4.2.2.1 Birth certificate</p> <p>4.2.2.2 National identity card</p> <p>4.2.2.3 Driving license</p> <p>4.2.3. The NDI solution including the enrolment software shall facilitate the collection of number of data/ information from citizens such as their name, address, gender, etc. This is yet to be finalized by the NSC.</p> <p>4.2.4. The employer will setup a verification center in order to verify data / information, scanned document collected from enrolment centers, prior releasing the information for personalization.</p> <p>4.2.5. The bidder shall ensure that the NDF centers are setup with relevant equipment and computing devices in order to achieve the above.</p> <p>4.2.6. The bidder shall provide adequate training for all the enrolment staff in and ensure that they are able to conduct the enrolment related activities and other related actions successfully.</p> <p>4.2.7. The bidder shall ensure a proper management center/ unit is setup in order to ensure successful management of bidder staff assigned to NDF centers for related tasks.</p> <p>4.2.8. The bidder shall ensure no interruptions will occur in any actions relevant / applicable to them.</p> <p>4.2.9. The bidder shall perform adequate tests to ensure all equipment are operating successfully and in compliance with the overall integration with the respective components of the centralized NDI solution.</p> <p>4.2.10. For each NDF center setup, the bidder shall obtain a UAT acceptance from the employer prior to commencing operations. The maximum duration of the above UAT is 1 month.</p> <p>4.2.11. The bidder shall obtain UAT certificate for equipment and computing hardware (project component applicable) located at each NDF center prior to</p>		

<p>the launch of the respective center.</p> <p>4.2.12. The bidder shall comply with the Warranty and Service Level Agreement(s)</p> <p>4.2.13. Once launched all NDF centers shall be managed in accordance with the Operational Manual, This shall indicate the responsibilities entrusted with the bidder. The bidder should comply with the responsibilities / actions mentioned in the above operations manual.</p>		
<p>4.3. [Item 2] – Portable Units</p>		
<p>4.3.1. The portable units shall be able to be successfully connected with the NDI platform / infrastructure.</p> <p>4.3.2. The portable units shall be able to be successfully integrated with the NDI solution, including the enrolment software.</p> <p>4.3.3. The NDI solution including the enrolment software shall facilitate the collection of above mentioned biometric data, scanned artifacts and citizens information.</p> <p>4.3.4. Each NDF center should be provided with a portal unit.</p> <p>4.3.5. The portable units will be utilizing to speed up the enrolment process and to reach citizens who are not able to visit the NDF centers.</p> <p>4.3.6. The portable unit shall be all inclusive single unit which can collect the above mentioned biometric data/information, scanned artifacts and citizen’s information via the enrolment software.</p> <p>4.3.7. The portable unit shall be easily carried, easily set-up and ready to use and all-in-one device.</p> <p>4.3.8. The bidder shall provide adequate training for all the staff and ensure that they are able to conduct the enrolment related activities and other aspects successfully.</p> <p>4.3.9. The bidder shall perform adequate tests to ensure the portable units are operating successfully and in compliance with the respective components of the centralized NDI solution.</p> <p>4.3.10. The bidder shall obtain UAT certificate for portable unit located at each NDF center, prior to the launch of the respective NDF center.</p> <p>4.3.11. The bidder shall comply with the Warranty and Service Level Agreement</p> <p>4.3.12. Once launched all NDF centers shall be managed in accordance with the Operational Manual, This shall indicate the responsibilities entrusted with the</p>		

<p>bidder including equipment and portable units. The bidder should comply with the responsibilities / actions mentioned in the above operations manual.</p>		
<p>4.4. [Item 3] - Centralized NDI Software Solution</p>		
<p>4.4.1. The centralized NDI software solution include among others, the NDI core, NDT platform, enrolment, NDI authentication services, services for lifecycle management.</p> <p>4.4.2. The NDI solution including the enrolment software shall facilitate the collection of the following biometric data.</p> <p>1.1.1.1. 2D Facial Image (Photo)</p> <p>1.1.1.2. finger prints (10)</p> <p>1.1.1.3. Iris scan</p> <p>4.4.3. The NDI solution including the enrolment software shall facilitate the collection of the following scanned images, among others,</p> <p>1.1.1.4. Birth certificate</p> <p>1.1.1.5. National identity card</p> <p>1.1.1.6. Driving license</p> <p>4.4.4. The NDI solution including the enrolment software shall facilitate the collection of number of data/ information from citizens such as their name, address, gender, etc. This is yet to be finalized by the NSC.</p> <p>4.4.5. The NDI solution, including the enrolment software needs to be designed and submitted for UAT acceptance.</p> <p>4.4.6. A centralized NDI software solution shall form the central repository of citizen’s digital data.</p> <p>4.4.7. The NDI solution shall comply with the overall NDI and NDT concept, envisioned by the government.</p> <p>4.4.8. The bidder shall ensure the NDI solution meet the all requirements including data capturing, verification and authentication aspects during project operation.</p> <p>4.4.9. The bidder shall ensure adequate / relevant functions are available in order for the enrolment data verification and translation staff to be able to function efficiently.</p> <p>4.4.10. The NDI solution shall comply with the functional requirements /specifications agreed with the employer, and specified under “7. Specifications”.</p> <p>4.4.11. The NDI solution shall comply with the non-functional requirements /specifications agreed with the employer, and specified under “7. Specifications”.</p>		

- | | | |
|---|--|--|
| <p>4.4.12. The bidder shall obtain UAT certification for the NDI solution prior to launching the solution.</p> <p>4.4.13. All aspects with regard to operational, support and maintenance of the NDI solution and its related integrations shall be specified and compliant in accordance with the Operational Manual signed between the employer and the bidder.</p> <p>4.4.14. The NDI solution shall be designed with features that provide flexibility and ease of future modification and expansion.</p> <p>4.4.15. The NDI solution shall be properly parameterized to facilitate future expansions and scalability.</p> <p>4.4.16. The client end of the NDI solution shall be portable to all standard and widely used web browsers. It shall be usable in all applicable computing devices taken in as part of this project.</p> <p>4.4.17. The NDI solution shall be a multi-user application where the application shall support multiple concurrent users to login and operate the application concurrently and simultaneously.</p> <p>4.4.18. The NDI solution shall support multi-tasking where the user must be able to perform multiple tasks without exiting the application. However, logical access control must be implemented so that the same user is unable to login to the system / application from more than one geographical location at the same time.</p> <p>4.4.19. The NDI solution shall maintain the concurrency of the database at all times irrespective of the number of user actions, tasks, or processes being simultaneously executed.</p> <p>4.4.20. The NDI solution shall have a Single-Sign-On (SSO) mechanism which will ensure that salient information and options are available to authorized users.</p> <p>4.4.21. The bidder shall provide appropriate tools for administering, monitoring and troubleshooting various software provided by them.</p> <p>4.4.22. The application must ensure data can be captured in trilingual (English/ Tamil and Sinhala).</p> <p>4.4.23. The NDI solution shall consist of workflows to ensure data captured can be verified against the documentation and any fields missed or needed to be updated can be edited.</p> <p>4.4.24. The NDI solution shall have a bill generation solution for each enrolment/ citizen registration.</p> <p>4.4.25. The NDI solution shall have adequate functions for the operator to generate a</p> | | |
|---|--|--|

check-out report and other related MIS reports to be generated via the centralized reporting module.

4.4.26. Overall concept of the NDI and NDT platform and the HTM solution

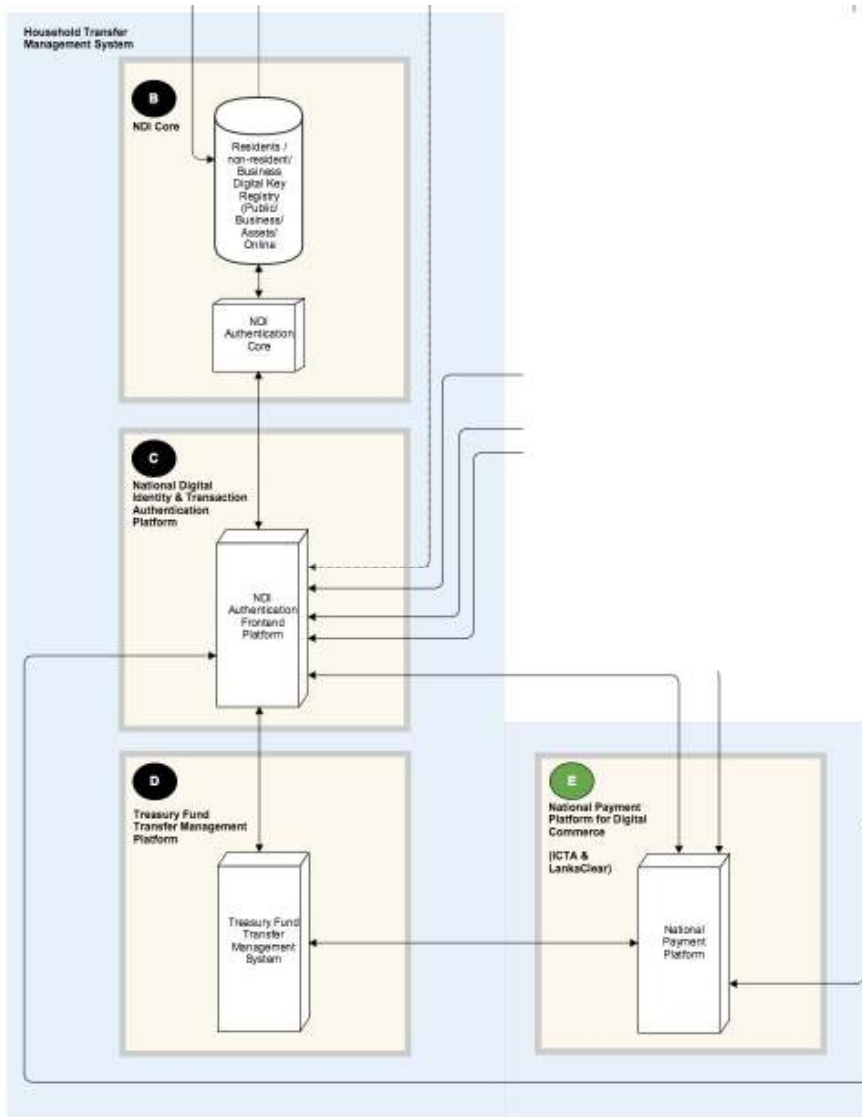


Figure 3: High-level view of the NDI and NDT platform and the HTM system

4.4.26.1 Above figure depicts component (B) NDI Core and (C) National Digital Identity Transaction (NDT) authentication platform and (D) Household Transfer Management (HTM) System for the Ministry of Finance.

4.4.26.2 Below is the high-level software architecture of the NDI Core and NDT Core.

4.4.26.3 The National Payment Platform (NPP), which has been marked as E (green color), has already been developed by ICTA and will be used to facilitate financial transaction.

4.4.27. (B) NDI Core and (C) NDT authentication platform can be further elaborated as follows.

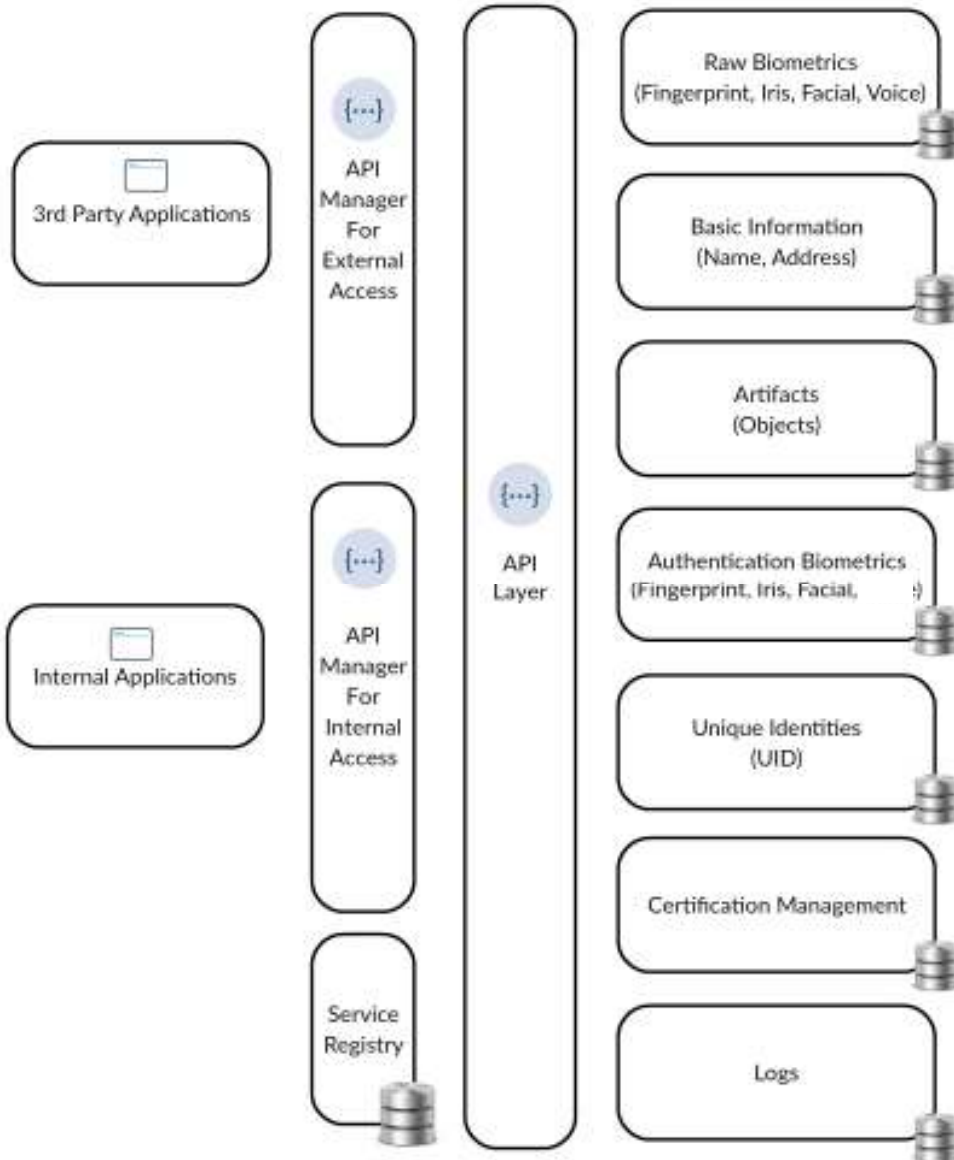


Figure 4: NDI core and NDT platform

4.4.27.1 Above architecture depicts the major components (Software Layer) of the National Digital Identity (NDI).

4.4.27.2 NDI contains several data-stores which are used to store citizen related information and biometrics. The data-stores can be listed as follows.

4.4.27.2.1 Raw biometrics – contains raw biometrics of the citizens

<p>which are collected during the time of the registration for the NDI. Fingerprints, Iris and Facial will be collected.</p>			
	4.4.27.2.2	<p>Basic information – contains the basic information of the citizens who are enrolled. Name, Address etc will be collected from the citizen. Please refer the data collected section of the diagram.</p>	
4.4.27.2.3	<p>Artifacts – contains scanned objects of the citizen such as photo, information of NIC, birth certificate will be as collected from the citizen. Please refer the data collected section of the diagram.</p>		
4.4.27.2.4	<p>Authentication biometrics - contains processed biometrics of the citizens that are used for authentication. Collected raw biometrics are converted using an algorithm which results processed biometrics.</p>		
4.4.27.2.5	<p>Public keys, Certificates – contains public keys, certificates of the citizens that are used for authentication and verifications. Public keys are generated through a personalization software during the time of registration that is used to issue smart cards to the citizens. Certificates will be provided by the NDI certification service provider</p>		
4.4.27.2.6	<p>Unique identities – contains unique strings and related information which are generated during the enrollment of the citizen. UID will be used across the data-stores to identify the citizen.</p>		
4.4.27.2.7	<p>Logs – contains logs related to National Digital Identity for audit purpose. Example would be access logs, authentication logs and biometric operations logs, smart card issuance, etc.</p>		
4.4.27.3	<p>The data-stores will be fronted by an API layer which consists server type of APIs.</p>		
4.4.27.3.1	<p>Data-store APIs - It is required to provide APIs for each and every data-store in order to access the information stored.</p>		
4.4.27.3.2	<p>Authentication APIs - it is required to provide APIs to authenticate a citizen based on the authentication biometrics that are stored. There are 4 levels of authentication services provided based on what you know, what you have and who you are.</p>		
4.4.27.3.2.1	<p>Authentication service that requires least security (smart</p>		

<p>card)</p> <p>4.4.27.3.2.2 Authentication service that requires multi/two factor authentication (smart card + OTP)</p> <p>4.4.27.3.2.3 Authentication service that requires multi/two factor authentication and digital signature (smart card + PIN)</p> <p>4.4.27.3.2.4 Authentication service that requires multi/three factor authentication and biometrics (smart card + PIN + biometrics)</p> <p>4.4.27.3.3 SSO API - it is required to provide API to be used for single sign on purpose.</p> <p>4.4.27.3.4 other related APIs - it is required to provide APIs to carry out other related operations of the NDI</p> <p>4.4.27.4 Above mentioned types of APIs will be exposed via an API layer to its stakeholders. These stakeholders are classified under two categories which are;</p> <p>4.4.27.4.1 Internal – NDI users who will be using the NDI application for data collection, smart card personalization and citizen authentication etc.</p> <p>4.4.27.4.2 External – 3rd party users such as digital instruction providers who would like to interact with the NDI to authenticate citizens.</p> <p>4.4.27.5 Therefore to demarcate the boundaries API layer is fronted by two API managers which serve internal and external stakeholders separately. All the API calls which are internal will be routed through internal API manager and All the API calls which are external will be routed through external API manager. The configuration or meta-data of the API managers will be stored in the service registry.</p> <p>4.4.27.6 API manager shall contain following features,</p> <p>4.4.27.6.1 API publishing</p> <p>4.4.27.6.2 Consuming APIs</p> <p>4.4.27.6.3 Routing API traffic</p> <p>4.4.27.6.4 Governing complete API lifecycle</p> <p>4.4.27.6.5 Monitoring and statistics</p> <p>4.4.27.6.6 Highly customizable</p> <p>4.4.27.6.7 Apply security</p> <p>4.4.27.6.8 High performance</p> <p>4.4.27.6.9 Scalable</p> <p>4.4.27.6.10 User-friendly graphical experience</p>		
--	--	--

- 4.4.27.7 Service registry shall contain following features,
 - 4.4.27.7.1 Registry & repository for meta data, policies etc
 - 4.4.27.7.2 SOA administration
 - 4.4.27.7.3 Configuration administration
 - 4.4.27.7.4 Manage & monitor
 - 4.4.27.7.5 User-friendly graphical experience
 - 4.4.27.7.6 Integrated with the API manager etc

- 4.4.27.8 Based on the APIs provided there can be two types of application
 - 4.4.27.8.1 Internal application
 - 4.4.27.8.1.1 Enrollment software that is used to enroll citizens to NDI.
At the time of registration citizen’s biometrics data will be captured and will be sent to relevant data-stores via APIs provided. After persisting the data in the data-stores data shall be made available to be accessed.
 - 4.4.27.8.1.2 Card personalization software that is used to issue cards to the citizens. At the same time key-pair will be generated by the application where public keys will be sent to the CSP along with the certificate signing requests (CSRs) for the issuance of digital certificates for the citizen.
 - 4.4.27.8.1.3 Lifecycle management software that is used to manage smart card after it has been issued. Citizen’s smart card related updates will be handled through this application.
 - 4.4.27.8.1.4 Quality assurance software that is used to ensure that the cards which have been issued are working as expected. In other words this software will verify the card is ready to be used by the citizen.
 - 4.4.27.8.2 3rd Party application - Any application that is authorized who are willing to interact with NDI.

4.4.28. Below architecture depicts the major components (Hardware Layer) of the National Digital Identity (NDI).

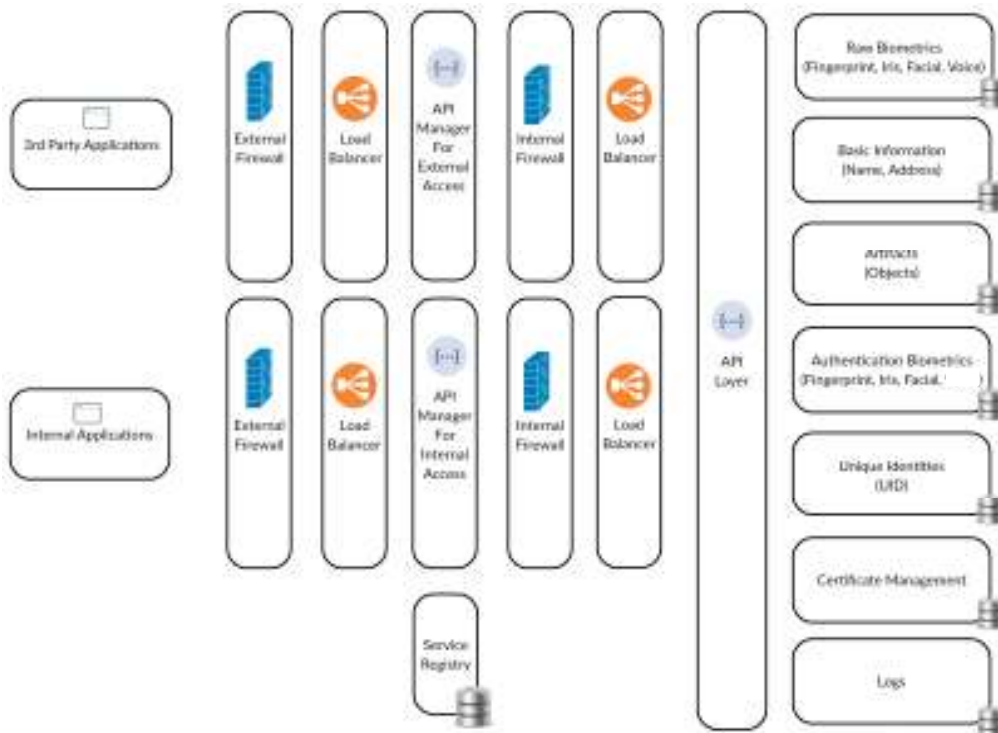


Figure 5: Major components (Hardware layer) of NDI

4.4.28.1 National Digital Identity infrastructure shall be scalable (scale-out) and highly available.

4.4.28.2 Non-functional requirements

4.4.28.2.1 Performance

4.4.28.2.1.1 Speed & Response Time

4.4.28.2.1.1.1 Minimum 1,000 authentications per second with response time less than 1 second based on NIC number

4.4.28.2.1.1.2 Minimum 1,000 authentications per second with response time less than 1 second based on User unique ID

4.4.28.2.1.1.3 Minimum 1,000 authentications per second with response time less than 1 second based on Finger prints

<p>4.4.28.2.1.1.4 Minimum 1,000 authentications per second with response time less than 1 second based on IRIS recognition</p>		
<p>4.4.28.2.1.1.5 Minimum 1,000 authentications per second with response time less than 1 second based on Face recognition</p>		
<p>4.4.28.2.1.1.6 Minimum 1,000 authentications per second with response time less than 1 second based on Digital key based authentication.</p>		
<p>4.4.28.2.2 Accuracy FAR or False Acceptance Rate is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a template. FRR or False Rejection Rate is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template CER or Crossover Error Rate is the rate where both accept and reject error rates are equal. FER The Failure to Enroll Rate (FER) is the percentage of the population which fails to complete enrollment.</p>		
<p>4.4.28.2.3 Availability System would be designed in a way to support high availability through clustering capabilities and maximum downtime < 1 hour</p>		
<p>4.4.28.2.4 Recoverability System shall be designed in a way to recover at any failure scenario with maximum downtime < 3 hrs</p>		
<p>4.4.28.2.5 Security System should be highly secured by following proper security configurations and industry standards.</p>		
<p>4.4.28.2.5.1 User authentication and authorization</p>		
<p>4.4.28.2.5.1.1 Username / password combination and any biometric information shall be used to validate the user before logged in to the system</p>		
<p>4.4.28.2.5.1.2 Access levels shall be maintained, in order to restrict the unauthorized access to the data.</p>		
<p>4.4.28.2.5.2 Storage</p>		
<p>4.4.28.2.5.2.1 Sensitive data shall be encrypted stored.</p>		

<p>Appropriate and strong encryption algorithms shall be used.</p> <p>4.4.28.2.5.3 Data Transmission</p> <p>4.4.28.2.5.3.1 HTTPS/SSL transport layer security shall be used and all the data shall be transferred via encrypted channel.</p> <p>4.4.28.2.6 Extensibility System shall be designed in a way to incorporate add-on modules of functionality to the application in production easily.</p> <p>4.4.28.2.7 Interoperability System shall be designed in a way to provide APIs which will allow any other applications to interact to this application easily.</p> <p>4.4.28.2.8 Localization Support for tri-lingual on data entry/query screens, in data fields, on reports, etc.; multi-byte character requirements; units-of-measure; currencies.</p> <p>4.4.28.2.9 Scalability System shall be designed to handle a wide variety of system configuration sizes or volumes in order to accommodate growth as per future requirement.</p> <p>4.4.28.2.10 Usability</p> <p>4.4.28.2.10.1 User Training</p>		
4.5 [Item 4] - Training of Enrollment Staff		
<p>4.5.1 The employer will to setup NDF data collection centers throughout the country.</p> <p>4.5.2 The enrollment officers located at each NDF center are responsible for carrying out the enrolment activities.</p> <p>4.5.3 In addition to the above, one portable unit is given to each of the DSs. The officers assigned to those unit are required for carrying out the enrolment activities.</p> <p>4.5.4 The bidder shall ensure that the above mentioned relevant staff involved in</p>		

	<p>the enrolment activities are fully trained and competent in carrying out their functions related to the enrolment and other related processes.</p> <p>4.5.5 In addition to the above the employer may assign other staff such as NDF center supervisors for the training programs, since they too should be fully trained.</p> <p>4.5.6 Therefore in order to achieve the above, the bidder shall develop a training plan, and carryout the training programs. The training programs should be in line implementation schedule.</p> <p>4.5.7 The bidder may use of the respective NDF centers to conduct respective training programs, or may use a suitable other location to carry out the trainings.</p> <p>4.5.8 The bidder shall undertake any costs associated with the training programs. This may include among others, training material, related devices, training center costs (if outside DSs), food, accommodation and travelling cost.</p> <p>4.5.9 The bidder shall conduct the training programmes prior to launching of the respective NDF centers.</p> <p>4.5.10 The bidder shall ensure relevant staff is fully and comprehensively trained in order to carry out all necessary relevant performances.</p> <p>4.5.11 Proof of training programs for the relevant staff, and a demonstration by enrolment staff shall be part of the requirement, which shall be full filled by the bidder during the UAT of a given NDF center.</p> <p>4.5.12 The overall training approach shall be presented to the Employer. And the training plan for each NDF center shall be agree upon by the respective NDF center manager / lead.</p> <p>4.5.13 The bidder shall ensure that the trainer and trainer assistants are competent and experienced in carrying out their respective tasks. They shall be subject specialist.</p> <p>4.5.14 The bidder shall ensure that the trainers and their assistants are having proven ability to deliver training programs in 3 languages i.e. based on the language competencies of each batch (Sinhala, Tamil and English).</p> <p>4.5.15 Provision of training shall include among others, resources (project managers, trainers, instructors, administration, logistics and quality inspectors) stationery, training guides, refreshments, utilities, training premises, parking facilities, computer equipment, peripherals, and accessories, training aids such as multimedia projectors and any other value additions that may be appropriate.</p> <p>4.5.16 Each training session shall be accessed by officers appointed by the</p>		
--	--	--	--

employer, to determine whether it has been a successful session.

4.5.17 The bidder shall comply with the “10. Implementation Schedule”

4.5.18 Training Modules/ sessions

4.5.18.1 Training sessions shall not be less than 7 hrs per-participant.

4.5.18.2 The bidder shall develop the content for all related modules. Bidder should specify clearly what the training modules are.

4.5.18.3 The participants to be given related training manuals. This needs to be specified.

4.5.18.4 Training manual content shall be prepared in three language. However a participant may require materials in one language.

4.5.18.5 The bidder shall ensure that the training sessions include practical sessions where hand-on training shall be given to educate the use of respective equipment, computing devices and the software solutions.

4.5.18.6 The bidder shall ensure the training manuals are comprehensive, there all aspects with regard to the enrolment process to be educated to staff. Thi9s may include among others, procedural and regulatory knowhow. The bidder shall work with the team appointed by the employer to advice, in order to refine these document to ensure completeness.

4.5.18.7 The bidder shall ensure that the detailed training plan is formulated and obtained approval from the Employer.

4.5.18.8 Training modules shall include the following among others;

4.5.18.8.1 General

4.5.18.8.1.1 Best practices about the use of ICT devices

4.5.18.8.1.2 Overall objectives about the project and the national initiative

4.5.18.8.1.3 Issues reporting/ resolution and the support procedure

4.5.18.8.2 Equipment used during the enrolment process

4.5.18.8.2.1 About the respective equipment

4.5.18.8.2.2 Use of equipment for data capturing

4.5.18.8.2.3 Ensuring the data is securely captured and stored / uploaded

4.5.18.8.3 Centralized software

4.5.18.8.3.1 About the software solution(s)

4.5.18.8.3.2 Use of the software solution(s)

4.5.18.8.3.3 Ensuring the data/ information is securely communicated via the software

4.5.18.8.3.4 Relevant operational functions and reporting

4.6 [Item 5] - Digital Transaction Cards (DTC) and Personalization

- 4.6.1 The Employer will setup NDF data collection centers throughout the country.
- 4.6.2 The bidder shall personalize both DTC (Phase 1) and DTC (Phase 2) cards.
- 4.6.3 The bidder shall be required to obtain approval from the employer for the design, features and other relevant aspects, prior to commencing manufacturing and operations.
- 4.6.4 The bidders shall carry out personalization of DTCs only at NDF district centers. There shall not be DTC personalization at DS centers. This operation shall be the responsibility of the bidder.
- 4.6.5 The number of digital personalizing units which the employer will locate at NDF district centers are indicated below;

Item	NDF district center types ->	A	B	C	D	DS centers
Digital card printing units		12	6	4	13	-

Table 4: DTC personalization

- 4.6.6 The bidder shall provide adequate staff to ensure SLAs are met for the cards personalization task.
- Night operations
- 4.6.7 However, with regard to DS NDF centers; the personalized DTCs will be issued only on the next working day. Therefore citizens who enroll from those DS locations are required to indicate at the time of enrollment whether they will collected their DTCs from the same DS, or from the District center. The bidder operations shall facilitate this process.
- 4.6.8 In a given district, personalization of DTCs of those who were enrolled via the DS centers of that district shall be carried out as night operation at respective NDF district centers.
- 4.6.9 However this is not a must. If there is time during the day time to print respective DTC, the bidder may do so, instead of the night operation, provided the day time operations are not interrupted, and the bidder meets the SLAs.
- 4.6.10 The night operations shall be conducted by the respective District NDF centers via the same cards personalization units

4.6.11 The bidder shall provide adequate staff to ensure the required maximum performances are met throughout the entire project period for the DTCs personalization activities and Quality Control / Quality Check units.

Dispatching of DTCs

4.6.12 Those DTCs QC passed for dispatch shall be handed over to the relevant officers appointed by the employer by the bidder's team at each NDF district center in an organized manner.

4.6.13 The bidder shall ensure the completion of the digital cards personalization in accordance with the SLA, in order to facilitate the distribution of the cards during the next day morning. This is also to ensure the day time operations are not interrupted.

4.6.14 In compliance with the implementation schedule, the bidder shall issue a DTC (Phase 1) card initially.

4.6.15 The bidder shall ensure that the DTCs are available for personalizing and to issue to citizens, in compliance with the implementation schedule.

4.6.16 DTC (Phase 2) should be designed, reviewed and ready for the final approval from the employer within 5 months of the effective date.

4.6.17 The employer will propose a mechanism to replace the (Phase 1) DTCs without interrupting the ongoing operational process. The bidder shall comply with the proposed approach with no additional cost to the employer.

4.6.18 In view of the objective of issuing the DTCs to citizens, for facilitating digital transactions, the bidder shall do the needful for obtaining relevant security and compliance certificates for the DTCs. Both local and international, if applicable.

4.6.19 The bidder shall obtain approval for, among others the design and layout of the DTCs with the relevant committee/ authority.

4.6.20 (If required), site visits to the DTC manufacturing plant shall be facilitated by the bidder during the approval process and periodic / ad-hoc audits deemed necessary by the employer. Bidder shall bear all associated costs. This is a determination needs to be made by the employers review committee.

4.6.21 The Employer will request DTCs in batches of 1,000,000 (1 Million) from the bidder. The bidder shall be able to successfully deliver the requested number of DTCs within 1 moth, from the date of the employer making the formal request.

4.6.22 Digital Transaction Cards personalization process

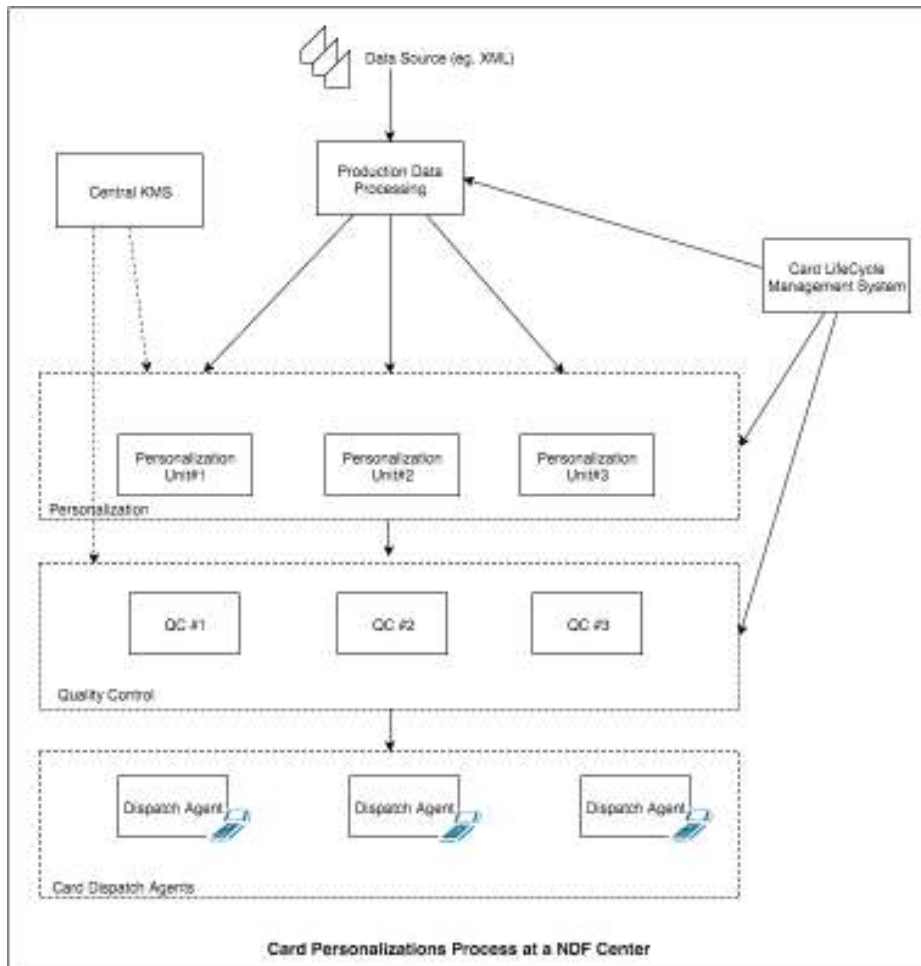


Figure 6: Card Personalization process

- 4.6.23 During the enrollment process, as a part of the verification procedure, a selected set of information captured above will be verified for accuracy and respective translations are entered real-time by the translation unit located at NDI Verification Center.
- 4.6.24 Once confirmed by the NDI verification center, it is possible to personalize the DTCs and to issue it to citizens.
- 4.6.25 Bidder shall support the employer set procedures for ensuring citizens will be able to collect their personalized DTCs from the NDF district centers prior to leaving the venue.
- 4.6.26 The NDF center operations shall be connected to central KMS (Key Management System).
- 4.6.27 The bidder shall ensure that all personalized cards shall go through a manual QC process before dispatching. Rejected cards are to be handled by the Card Lifecycle Management system.

<p>4.6.28 The bidder shall ensure that a Card Lifecycle Management is implemented at NDF district centers.</p>		
<p>4.6.29 The digital card personalization should be fully automated.</p>		
<p>4.6.30 The bidder shall be fully responsible for the DTC personalization unit located at each NDF center.</p>		
<p>4.6.31 The bidder shall specify the related functions at this unit clearly, and the required space.</p>		
<p>4.6.32 Card lifecycle management system</p>		
<p>4.6.32.1 The system shall be flexible to enable easy upgrading in the future.</p>		
<p>4.6.32.2 The system shall be operational on any standard hardware.</p>		
<p>4.6.32.3 The system shall be based on web application model and java object oriented software conforms to J2EE.</p>		
<p>4.6.32.4 Scalability and high performance: Card lifecycle management system shall be scalable to provide high performance and to ensure business continuity.</p>		
<p>4.6.32.5 Extendibility: Card lifecycle management system shall be designed in a modular architecture to add new products, new application with minimum impact on the solution.</p>		
<p>4.6.32.6 Software modules can integrate securely and easily with external systems such as enrolment system, National registry, Certification Service Provider, Card Personalization center, Post-Issuance system.</p>		
<p>4.6.32.7 Graphical User Interface (GUI) shall be easy to use and it shall provide a simple interface for managing processes and configuration.</p>		
<p>4.6.32.8 The system architecture shall be designed to present 4 layers:</p>		
<p>4.6.32.8.1 Persistency layer: Secure the persistence of the data.</p>		
<p>4.6.32.8.2 Business logic layer: containing business entities /modules to manage the services/features of the card lifecycle management system such as data processing, stock management, and document/card lifecycle.</p>		
<p>4.6.32.8.3 Orchestration layer; providing a workflow engine enabling to connect any components of the boundary layer to a business logic modules</p>		

<p>4.6.32.8.4 Boundary layer: Providing GUI, gateways and connectors to interface the external entities/systems. It shall be composed of a following;</p> <p>4.6.32.8.4.1 Web server that will handle the business logic management and manage easily the connection to external system (Enrolment Management System, Registry, Certificate Authority, Post-Issuance server)</p> <p>4.6.32.8.4.2 A client GUI, for the user to</p> <p>4.6.32.8.4.2.1 Manage product, application and card personalization center configuration</p> <p>4.6.32.8.4.2.2 Monitor the activity</p> <p>4.6.32.8.4.2.3 Generate customized production report</p> <p>4.6.32.8.4.2.4 Manage the inventory</p> <p>4.6.32.9 Card lifecycle management system shall be capable to provide the following services:</p> <p>4.6.32.9.1 Lifecycle services: manage shipped/delivered/hand out/lost/stolen/damage/end of life status</p> <p>4.6.32.9.2 Data preparation for both issuance and post issuance for all the application managed by the card lifecycle management system.</p> <p>4.6.32.9.3 Consultation: provide access to Biometric info from fixed or mobile stations for officers</p> <p>4.6.32.9.4 SMS notification: provide a way to send SMS to citizens (notification for card collection, for renewing certificates, for managing pin code)</p> <p>4.6.32.10 Card lifecycle management system shall be capable to manage following functions</p> <p>4.6.32.10.1 Card, application and request management</p> <p>4.6.32.10.1.1 Register and control the lifecycle of the card, the card application and the request from the pre-personalization to card expiration and destruction.</p> <p>4.6.32.10.1.2 Handle, stores, and update all information about cards and application status, personal information in the database</p> <p>4.6.32.10.1.3 New product definition shall be configurable through the GUI (product profile, applications, applets)</p> <p>4.6.32.10.1.4 New application definition and linkage to product shall be configurable through the GUI</p> <p>4.6.32.10.2 Materials and stock management</p>		
---	--	--

<p>4.6.32.10.3 Support multiple sites</p> <p>4.6.32.10.3.1 Different card storage shall be able to configured and assigned to production center.</p> <p>4.6.32.10.3.2 Track the cards status</p> <p>4.6.32.11 Card lifecycle management system shall be capable to manage following functions</p> <p>4.6.32.11.1 Card Personalization Order</p> <p>4.6.32.11.1.1 System shall be able to manage card personalization orders and the process of sending card personalization orders to the card production center.</p> <p>4.6.32.11.1.2 The system shall be able to handle several card issuance centers simultaneously</p> <p>4.6.32.12 Card lifecycle management system shall be able to handle multiple products (ie: smart card products) simultaneously.</p> <p>4.6.32.13 Card lifecycle management system shall be able to handle user account management function to ensure that a certain operator is allowed to do only certain work phases</p> <p>4.6.32.13.1 Access rights shall be based on roles of operator, auditor, and administrator.</p> <p>4.6.32.13.2 Specific rights shall be configurable for each role.</p> <p>4.6.32.14 This system shall be ready and open for different type authentication methods (LDAP).</p> <p>4.6.32.15 Card lifecycle management system shall be able to handle reporting</p> <p>4.6.32.15.1 Reports shall be generated on any information stored in the database</p> <p>4.6.32.15.2 Reporting system shall be customizable</p> <p>4.6.32.16 Card lifecycle management system shall be able to handle auditing</p> <p>4.6.32.16.1 The system shall enable logging of each step containing information about the operator, time and data for audit purposes (visible only by an auditor profile).</p> <p>4.6.32.16.2 The system log shall ensure the log integrity.</p> <p>4.6.32.17 Card lifecycle management system shall be able to handle security and confidentiality</p> <p>4.6.32.17.1 Communication with external systems shall be secured using Strong TLS with mutual authentication</p>		
---	--	--

(client/server)

- 4.6.32.17.2 Sensitive data stored in the database shall be encrypted.
- 4.6.32.18 Search functions for authorized operators /systems shall be implemented at requests and cards level.
- 4.6.32.19 The system shall implement bi directional connectors to easily communicate with the following external systems:
- 4.6.32.19.1 National registry
 - 4.6.32.19.2 Certification Service Provider of the NDI
 - 4.6.32.19.3 Perso-centers (personalization centers)
 - 4.6.32.19.4 Post issuance facilities
 - 4.6.32.19.5 SMS center
- 4.6.33 Post issuance solution
- 4.6.33.1 The bidder shall already have strong prior experience of minimum 2 post issuance solution deployment with more than 2000 post issuance points.
- 4.6.33.2 The proposed solution shall be platforms agnostic and deployable on multiple platforms (operating systems & browsers environments):
- 4.6.33.2.1 Internet Explorer
 - 4.6.33.2.2 Mozilla Firefox
 - 4.6.33.2.3 Google Chrome
 - 4.6.33.2.4 Safari
- 4.6.33.3 Interface shall be user-friendly & no end-user configuration needed.
- 4.6.33.4 Post issuance shall be made possible through internet within:
- 4.6.33.4.1 Web-based interface available through a personal computer or a kiosk (Self-service) for user.
 - 4.6.33.4.2 In both cases no software deployment shall be required on kiosks / personal computer. A card reader and browser shall be sufficient.
- 4.6.33.5 Post issuance shall be available for the following elements:
- 4.6.33.5.1 Card attributes update (i.e.: change of address)
 - 4.6.33.5.2 Certificate loading / renewal
 - 4.6.33.5.3 Pin change/unblock
 - 4.6.33.5.4 Application loading
- 4.6.33.6 The proposed solution shall help to prevent common threats from the Internet, such as:
- 4.6.33.6.1 Man in The Middle attacks
 - 4.6.33.6.2 Protocol attacks
 - 4.6.33.6.3 Phishing
 - 4.6.33.6.4 Pharming.
 - 4.6.33.6.5 OWASP top 10

4.7 [Item 6] - NDI Hosting Infrastructure

- 4.7.1 The Employer will provide an ICT infrastructure facility to host the entire system with highly available and high performance hardware.
- 4.7.2 There will be two sites;
 - Live data center facility I
 - Live data center facility II
- 4.7.3 The bidders shall comply with the “6. Schedule of Requirement”.
- 4.7.4 The bidders shall comply with the “7. Items Specifications”.
- 4.7.5 Solution overview

Item No	Software Component	Description	Software In Scope Yes/No	Bidder to provide infrastructure
4.7.5.1	Enrolment Front-End	Software solution accessed via enrolment stations located throughout the country.	Yes	Yes
4.7.5.2	Authentication Front-End	Software solution used for biometric and other personal identification data authentication during operations.	Yes	Yes
4.7.5.3	Enrolment Application	Back End Solution to manage the enrolment data	Yes	Yes
4.7.5.4	Authentication System	Back End Solution to manage the authentication.	Yes	Yes
4.7.5.5	Database / Storage	To store enrolment biometric and other personal identification data	Yes	Yes
4.7.5.6	Management	Infrastructure management, monitoring, transaction and system log analyzing.	Yes	Yes
4.7.5.7	Backup System	Management of systems backups	Yes	Yes

4.7.6 Proposed structure for the production sites

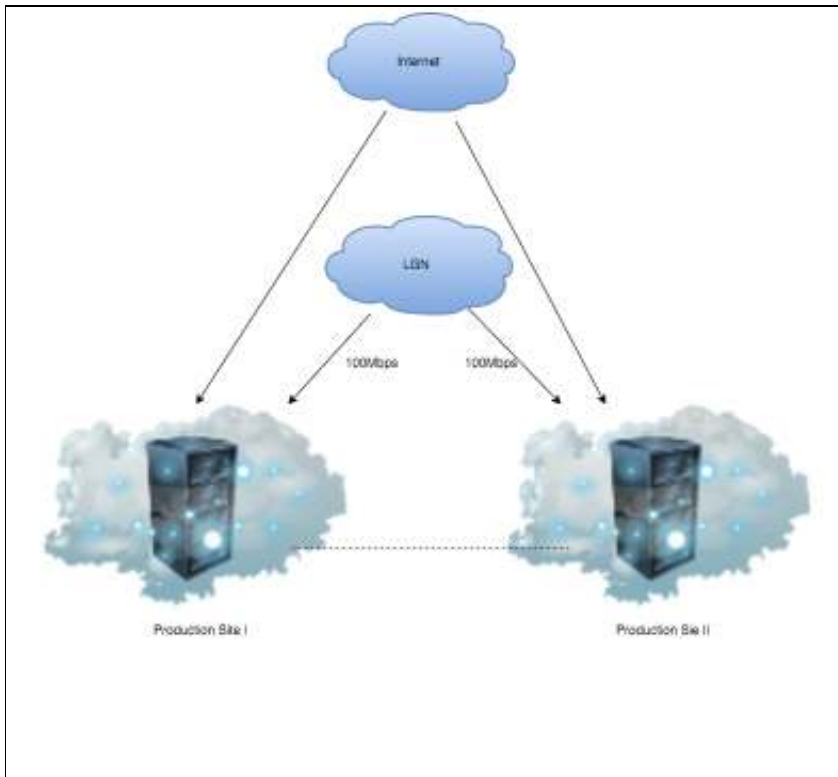


Figure 7: Proposed structure for the production site

4.7.7 Production datacenter I and II

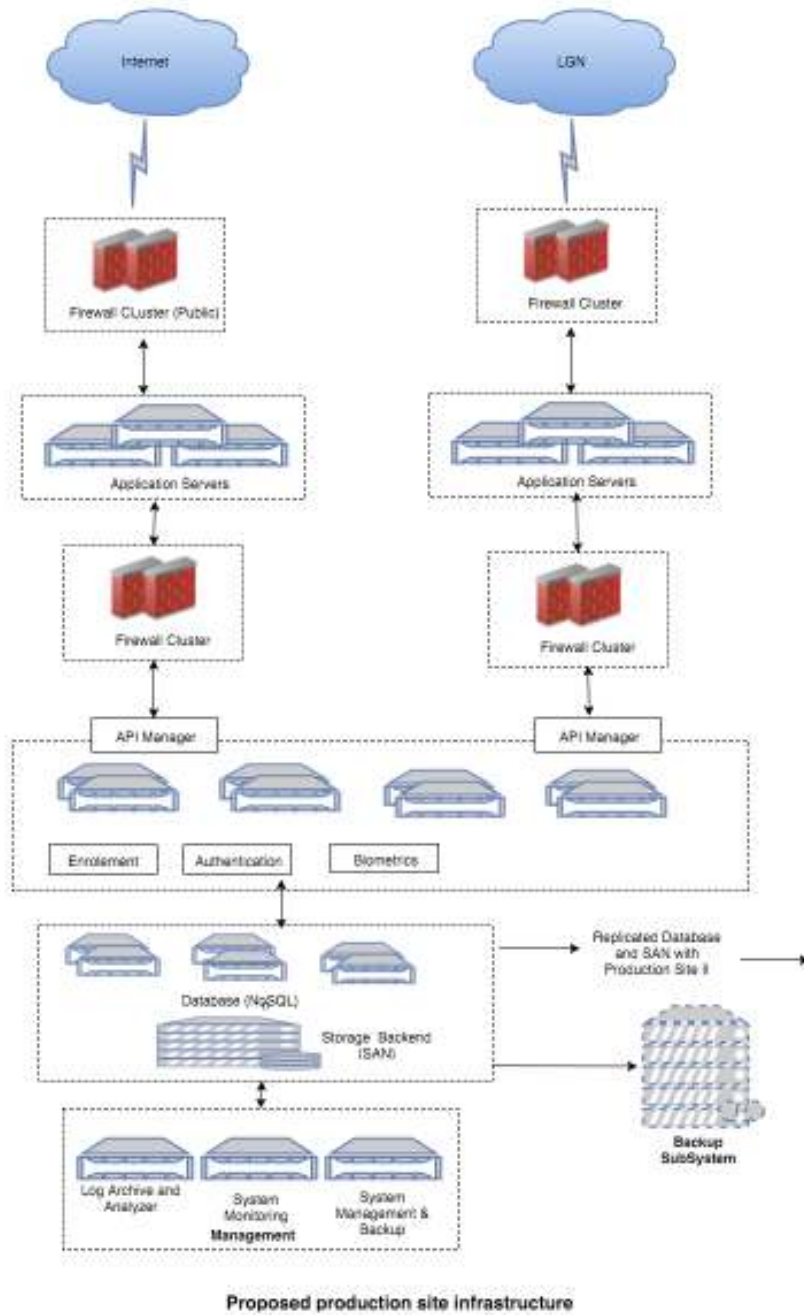


Figure 8: Production Data Center I & II

4.8 [Item 7] - NDI Certification Service Provider (Certification Authority) and Services

4.8.1 NDI Certification Authority.

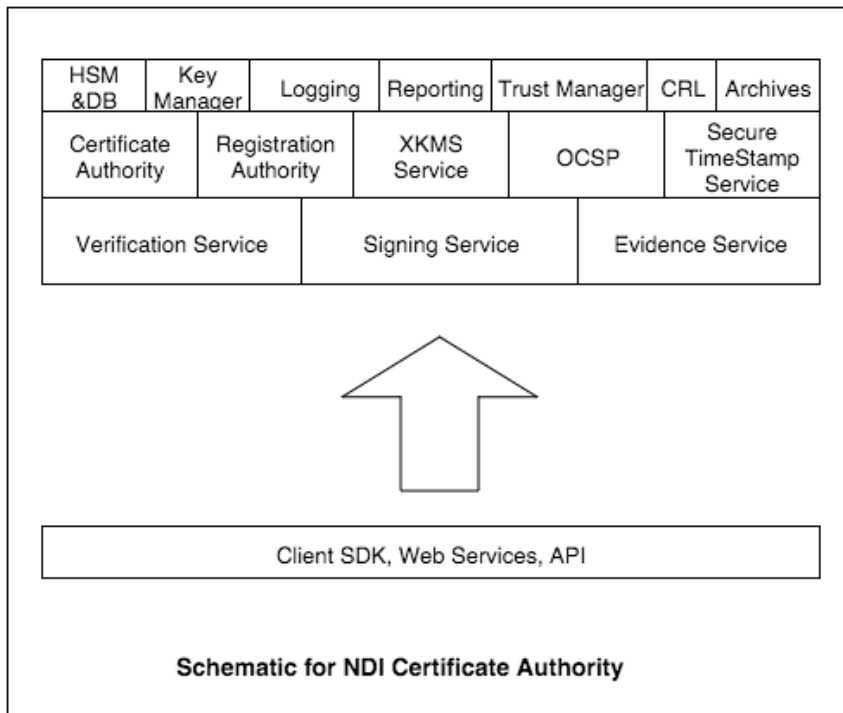


Figure 9: Schematic for NDI Certificate Authority

4.8.2 NDI Certification Service Provider (NDI CSP) to be established under the National Certification Authority (NCA), which provides the Public Key Infrastructure (PKI) for the entire NDI platform.

4.8.3 NDI CSP shall offer the certificate lifecycle services for citizen’s digital certificates.

4.8.4 PKI Platform shall be highly available (HA) and DR shall be facilitated.

4.8.5 Role based access control for all system services.

4.8.6 NDI CSP comprises of the services CA, RA, Time Stamp Authority (TSA) OCSP /CRL, XKMS. On top of above Signing, Validation and Evidence services shall be established.

4.8.6.1 NDI CA core shall CWA 14167-1 compliant, supports x.509 v3, EV(DV,OV) Certificates

4.8.6.2 CA, RA must support

4.8.6.2.1 Pre-production smart cards, tokens and it shall support issuance of certificate to smart cards, tokens, soft(PKCS#12) and mobile devices.

	<p>4.8.6.2.2 Store CA keys in HSM.</p> <p>4.8.6.2.3 Issuance of x.509 certificate based on CSR.</p> <p>4.8.6.2.4 Multiple, parallel working of operators.</p> <p>4.8.6.2.5 Notifications through e-mail and SMS.</p> <p>4.8.6.3 OCSP responder shall be</p> <p>4.8.6.3.1 RFC 6960, RFC 5019 compliant.</p> <p>4.8.6.3.2 Able to manage and configure via web interface.</p> <p>4.8.6.3.3 Logging all transactions.</p> <p>4.8.6.3.4 Able to provide comprehensive reporting and exporting data.</p> <p>4.8.6.4 TSA shall compliant RFC3161 and supports up to 4096-bit RSA and SHA-512 fingerprints.</p> <p>4.8.6.5 TSA shall support CADES, PAdES Part 4, IETF LTANS ERS (RFC 4998 ERS, RFC4810) timestamp and archive services.</p> <p>4.8.6.5.1 CA services shall be available via APIs for the third NDI core applications (Smartcard personalization, authentication).</p> <p>4.8.6.5.2 NDI CSP shall be WebTrust 2.0 (or latest) compliant and highest possible security shall be established. It shall have WebTrust seal issued by CPA Canada annually.</p>		
4.9 [Item 8] - Household Transfer Management (HTM) system			
<p>4.9.1</p>	<p>Introduction</p> <p>Household Transfer Management (HTM) system is a collection of software systems which functions together to facilitates the management of fund transfers /fund disbursements initiated by Treasury department of the Ministry of Finance to beneficiary or beneficiary group(s) under Social welfare and Safety-net programs, Pensions and other specified citizen groups .</p>		

- 4.9.2 The high-level conceptual view of the household transfer management (HTM) system integrating with key components such as the NDI authentication service, and the National Payment Platform (NPP) are indicated below;

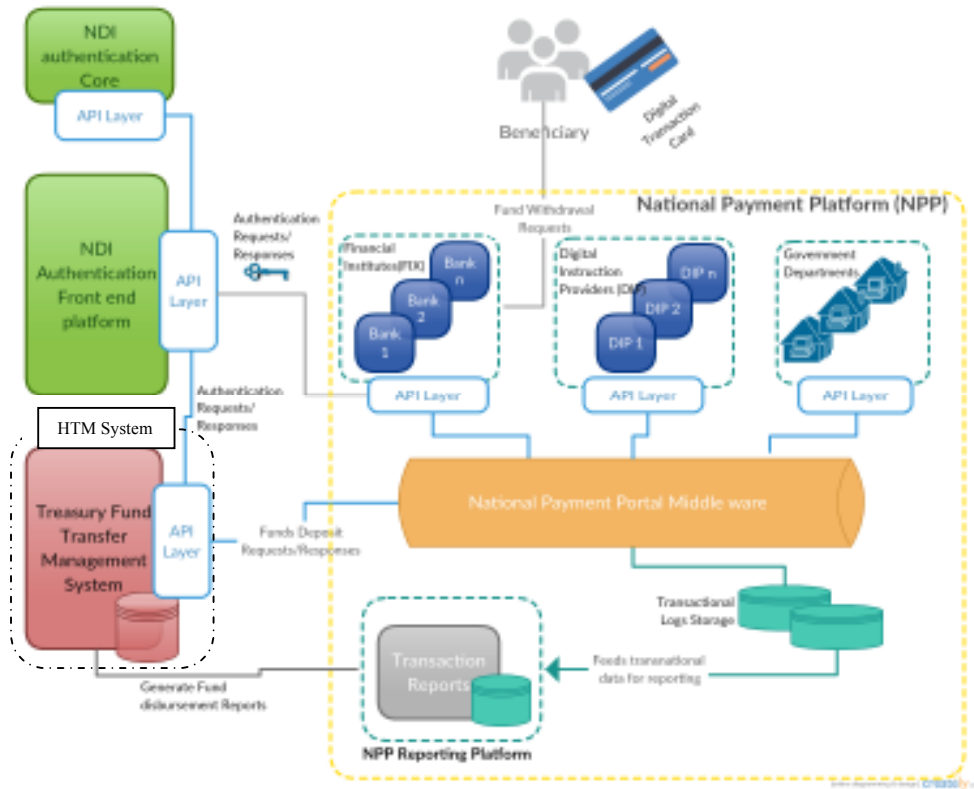


Figure 10 : High-level conceptual view of the HTM system

- 4.9.3 As Figure-01 depicts, the HTM uses a collection of components which facilitate the fund transfer to beneficiary.
- 4.9.4 The bidder should facilitate the integration with the following;
- 4.9.4.1 National Digital Identity and Transaction Authentication Platform.
Facilitates the unique identification of a beneficiary in digital space and authenticate the beneficiary using artifacts of the beneficiary such as UID, digital keys, OTP, Biometric information etc. prior initialization of a transaction
- 4.9.4.2 National Payment Platform (NPP)
The government transaction platform for facilitating direct transfer of funds to beneficiary accounts. And also authorized financial institutes and Digital instruction providers are

connected with NPP in order to facilitate real time transactions. The employer will provide the NPP platform.

4.9.5 Adherence to SOA and good governance principals, all these platforms are loosely-coupled and interoperable in their nature. The communication among these platforms will be done through a set of common rest APIs which provided by each and every platform to access their functionalities. Therefore, back-end integration with the existing fund management system to these platform will be easy and straight forward.

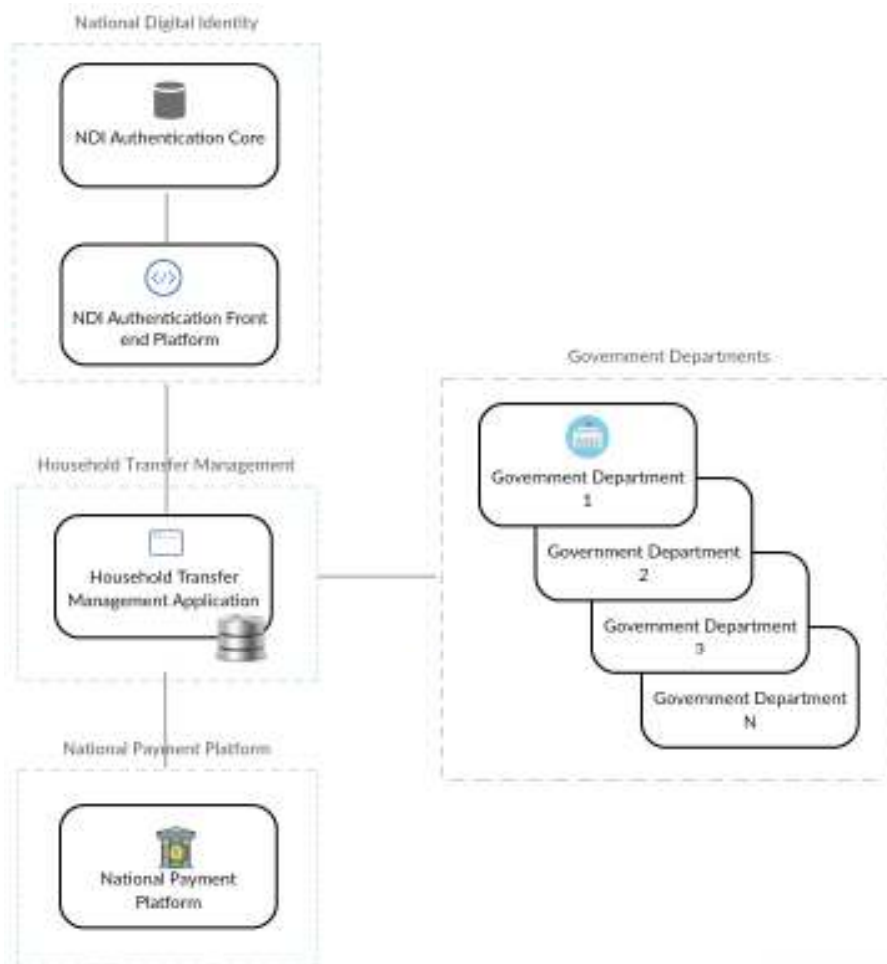


Figure 11: High level architecture of the HTM system implementation

4.9.6 Above diagram depicts household transfer management (HTM) system architecture.

4.9.6.1 A government department will request HTM module to disburse funds to its beneficiaries.

4.9.6.2 Household transfer management application shall consist a Business Rules Management System (BRMS). Once there is a request for disbursement application will execute the business rules against the request to make sure beneficiaries are authentic (including the NDI verification).

4.9.6.3 Once the verification is completed the payment disbursement request will be sent to National Payment Platform (NPP) for the disbursement of funds.

4.9.7 Key Features

The key features of the fund transfer module are as follows;

4.9.7.1 Facilitate fund transfers/withdrawals from/to beneficiary's bank account by integrating to the NPP.

4.9.7.2 Real-time fund transfer/withdrawal tracking

4.9.7.2.1 Via real time status updates

4.9.7.2.2 Reporting

4.9.7.3 Fund Transfers

4.9.7.3.1 It is mandatory to beneficiary to having a bank account in a bank which is integrated to National Payment Portal (NPP) prior fund transfer through fund transfer module.

4.9.7.3.2 Treasury fund transfer management system authenticate the beneficiary information via NDI & Transaction authentication platform using biometrics and obtain the public key of the beneficiary.

4.9.7.3.3 Beneficiary's bank account number or any other sensitive information will be not used/sent but the UID of the beneficiary will be sent to the NPP along with the fund transfer request.

4.9.7.3.4 At NPP, UID to Account number mapping will be maintained. Therefore, using the UID, the beneficiary account will be identified and fund transfer will be done.

4.9.7.3.5 Status of the fund transfer will be notified (real-time) to the treasure fund management system by the bank through NPP.

<p>4.9.7.4 Real-time fund transfers tracking</p> <p>4.9.7.4.1 Real - time status update</p> <p>4.9.7.4.1.1 Upon fund transfer/withdrawal happens, the fund management system will be updated through NPP.</p> <p>4.9.7.4.1.2 Therefore, at a given time, the fund management system demonstrates the true status of the fund disbursement.</p> <p>4.9.7.4.2 Reporting</p> <p>4.9.7.4.2.1 As the Figure-1.0 depicts, all the fund transfer/withdrawal requests and responses are routed through NPP middle-ware infrastructure. The middle-ware contains transaction logs storages to logged all the transaction requests/responses.</p> <p>4.9.7.4.2.2 These logs will be used to generate the verity of transaction reports which can be used for decision making.</p> <p>4.9.7.4.2.3 Via the NPP reporting platform, Department of Treasury Operations can generate transactional reports relevant to the fund transfer and verity of status reports.</p> <p>4.9.7.4.2.4 These reports can be used to track the real time fund transfer/withdrawal statuses.</p>		
--	--	--

4.10 Review Committees and Review Procedures

4.10.1 All deliverables will be reviewed by the team appointed by the National Steering Committee (NSC) established for this project.

5 Warranty and Service Level Agreement (SLA)

5.1 [Item 1] - Enrolment Stations

5.1.1 Warranty Requirements

- 5.1.1.1 The warranty period shall be sixty months (60 months) comprehensive on-site bidder authorized warranty (Labor and Parts) with one to one backup in case workshop attention is required for all Notebooks, Printers, Scanners, POS printers, USB Hubs, LED Monitors, Condenser Mic's, Camera's, Finger print scanners, Iris scanners and portable biometric collection kits.
- 5.1.1.2 60 months comprehensive on-site warranty shall commence from the Acceptance of the goods by the employer.
- 5.1.1.3 For purposes of the Warranty, "on-site" is the place (s) of final destination sites specified by the employer.
- 5.1.1.4 For purposes of the Warranty, "on-site" means Bidder shall allocate adequate staff to visit the site to identify the problem and resolve the problem in coordination with employer.
- 5.1.1.5 Annually One (1) dedicated preventive maintenance service shall be provided by the bidder during the period of warranty and submit completion report to employer.
- 5.1.1.6 The Bidder must maintain spare parts stock for repairs and replacements for the duration of the warranty service period.
- 5.1.1.7 The Bidder must bear all charges with regard to the supply of spare parts, labor, travel, per diem and accommodation to the bidder staff etc; during the period of warranty. Employer will NOT pay any additional expenditure for services rendered during the warranty period.

5.1.2 Service Level Agreement (SLA)

The aim of this agreement is to provide a basis for close co-operation between the employer and the bidder for support and maintenance services to be provided by the Bidder, thereby ensuring a timely and efficient support service is available.

5.1.3 Objectives of Service Level Agreements

- 5.1.3.1 To create an environment conducive to a co-operative relationship between Employer, bidder and Employer's representatives (government organizations) to ensure the effective support of all end users.
- 5.1.3.2 To document the responsibilities of all parties taking part in the Agreement.
- 5.1.3.3 To define the commencement of the agreement, its initial term and the provision for reviews.

- 5.1.3.4 To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.
- 5.1.3.5 To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
- 5.1.3.6 To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.
- 5.1.3.7 To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

5.1.4 The Warranty Support SLA is mentioned below;

5.1.4.1 Warranty Support SLA 1

Incident Management / Resolution	Live Data Center
Response for Resolution	
Critical Incident Response	1 hr
Major Incident Response	2 hrs
High Incident Response	4 hrs
Time to Fix	
Critical Incident	8 hrs
Major Incident	10 hrs
High Incident	12 hrs

5.1.4.2 Warranty Support SLA 2

Severity Level	Description	Type of Issues / incident
Critical (24x7)	Enrolment staff cannot function	Any device issue/ fault at enrolment centers
Major (8:00 a.m. to 5:00 p.m.)	NDF center functions at degraded performance	Any device issue/ fault at enrolment centers
High (8:00 a.m. to 5:00 p.m.)	NDF center functions at degraded performance	Portable biometric data collection device issue

5.1.5 Penalties

If problems are not corrected within the time limit specified (Response + Resolution time in Warranty support SLA 1), the employer will be entitled to a penalty payment as specified below for each day that the bidder fails to resolve the problem.

5.1.5.1 Critical : LKR 50,000/- per hour

5.1.5.2 Major : LKR 40,000/- per hour

5.1.5.3 High : LKR 30,000/- per hour

5.1.5.4 Maximum LKR 300,000.00 per incident

5.1.5.5 Maximum penalty per year is LKR 3,000,000.00.

INSPECTION COPY

5.2 [Item 2] – Portable Units

5.2.1 Warranty Requirements

- 5.2.1.1 The warranty period shall be sixty months (60 months) comprehensive on-site bidder authorized warranty (Labor and Parts) with one to one backup in case workshop attention is required for all portable biometric collection kits.
- 5.2.1.2 60 months comprehensive on-site warranty shall commence from the Acceptance of the goods by the Employer.
- 5.2.1.3 For purposes of the Warranty, “on-site” is the place(s) of final destination sites specified by the employer
- 5.2.1.4 For purposes of the Warranty, “on-site” means Bidder shall allocate adequate staff to visit the site to identify the problem and resolve the problem in coordination with employer
- 5.2.1.5 Annually One (1) dedicated preventive maintenance service shall be provided by the bidder during the period of warranty and submit completion report to employer.
- 5.2.1.6 Bidder must maintain spare parts stock for repairs and replacements for the duration of the warranty service period.
- 5.2.1.7 Bidder must bear all charges with regard to the supply of spare parts, labour, travel, per diem and accommodation to bidder staff etc; during the period of warranty. Employer will NOT pay any additional expenditure for services rendered during the warranty period.

5.2.2 Service Level Agreement (SLA)

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

5.2.3 Objectives of Service Level Agreements

- 5.2.3.1 To create an environment conducive to a co-operative relationship between Employer, bidder and Employer's representatives (government organizations) to ensure the effective support of all end users.
- 5.2.3.2 To document the responsibilities of all parties taking part in the Agreement.
- 5.2.3.3 To define the commencement of the agreement, its initial term and the provision for reviews.
- 5.2.3.4 To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.

- 5.2.3.5 To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
- 5.2.3.6 To provide a common understanding of service requirements /capabilities and of the principals involved in the measurement of service levels.
- 5.2.3.7 To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

5.2.4 The Warranty Support SLA is mentioned below;

5.2.4.1 Warranty Support SLA 1

Incident Management / Resolution	Live Data Center
Response for Resolution	
Critical Incident Response	1 hr
Major Incident Response	2 hrs
Time to Fix	
Critical Incident	8 hrs
Major Incident	10 hrs

5.2.4.2 Warranty Support SLA 2

Severity Level	Description	Type of Issues / incident
Critical (24x7)	Enrolment staff cannot function	Any component issue/ fault in portable unit
Major (8:00 a.m. to 5:00 p.m.)	NDF center functions at degraded performance	Any component issue/ fault in portable unit

5.2.5 Penalties

If problems are not corrected within the time limit specified (Response + Resolution time in Warranty support SLA 1), the employer will be entitled to a penalty payment as specified below for each day that the bidder fails to resolve the problem.

- 5.2.5.1 Critical : LKR 50,000/- per hour
- 5.2.5.2 Major : LKR 40,000/- per hour
- 5.2.5.3 Maximum LKR 300,000.00 per incident
- 5.2.5.4 Maximum penalty per year is LKR 3,000,000.00.

INSPECTION COPY

5.3 [Item 3] – Centralized NDI Software Solution

5.3.1 Introduction

The aim of this agreement is to provide a basis for close co-operation between the Employer and the Bidder for support and maintenance services to be provided by the Bidder, 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.

5.3.2 Objectives of Service Level Agreements

- 5.3.2.1 To create an environment conducive to a co-operative relationship between Employer, Bidder and Employer's representatives (government organizations) to ensure the effective support of all end users.
- 5.3.2.2 To document the responsibilities of all parties taking part in the Agreement.
- 5.3.2.3 To define the commencement of the agreement, its initial term and the provision for reviews.
- 5.3.2.4 To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.
- 5.3.2.5 To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
- 5.3.2.6 To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.
- 5.3.2.7 To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

5.3.3 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.

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 Employer and Bidder. In the event of a discrepancy between actual and targeted service levels both Employer and Bidder are expected to identify and resolve the reason(s) for any discrepancies in close co-operation.

Service level monitoring will be performed by Employer. Reports will be produced as and when required and forwarded to the Bidder.

5.3.4 Support Levels

The bidder must provide support and maintenance services during Support Levels mentioned below;

Support Level 1 : High	
Component/ Service	Centralized NDI Solution
Support Hours	24 hours a day, all days in the week (including public and mercantile holidays)
Support Level 2 : Medium	
Component/ Service	NDI solution interfaces accessed via NDF centers.
Support Hours	From 08:30 AM to 05:30 PM Monday to Friday (excluding public holidays)

5.3.4.1 SLA applicable during the services and maintenance period, applicable as the UAT certificate is issued: Support Level 1 and 2.

5.3.5 On-Call Services Requirements

Bidder must make at least one qualified personnel available to the Employer by telephone, email and issue tracking system for the reporting and resolution of non-conformities or other issues, defects or problems.

Dedicated telephone numbers, emails, tracking system shall be available for reporting issues.

Employer will nominate the personnel who are authorized to report non-conformities or other problems with the system. Reporting of non-conformities includes requests by the Employer to apply critical software updates or patches.

Table-1 shows the response priority assigned to faults according to the perceived importance of the reported situation and the required initial response times for the individual priority ratings. All times indicated represent response time during specified Support Levels.

The indicated response time represents the maximum delay between a fault /request being reported and a Bidder's representative contacting the Employer by telephone.

The purpose of this contact is to notify the Employer of the receipt of the fault /request and provide the Employer with details of the proposed action to be taken in respect of the particular fault /request.

Support Level	Business Critical		Non-Business Critical	
	Fatal	Impaired	Fatal	Impaired
High	60 minutes within Support Hours	90 minutes within Support Hours	90 minutes within Support Hours	120 minutes within Support Hours

Table-1: Response Priority

Note:

- Fatal - Total system inoperability
- Impaired - Partial system inoperability
- Business Critical - Unable to perform core business functions
- Non-Business Critical - Able to perform limited core business functions

Furthermore, time to resolve the Problem, is support level time, starting from the actual time of receiving the bidder notification. However if the notification is occurred outside the defined support level time, then time to resolve the Problem, is support level time, starting from as the next support level begins.

5.3.6 Problem Resolution and Penalties

If faults are not corrected within the time limits specified in the Table-2, the Employer will be entitled to a penalty payment for each hour that the Bidder fails to resolve the fault.

Support Level	Business Critical		Non-Business Critical	
	Fatal	Impaired	Fatal	Impaired
High	6 Hours LKR 100,000.00 per hour	10 Hours LKR 100,000.00 per hour	10 Hours LKR 100,000.00 per hour	15 Hours LKR 100,000.00 per hour

Table-2: Resolution Time and Penalties

5.4 [Item 5] – Digital Transactions Card (DTC) and Personalization

- 5.4.1 The bidder shall provide adequate staff to ensure SLAs are met for DTC (Phase 1 and phase 2 cards) personalization.
- 5.4.2 The bidder shall ensure the completion of the digital cards printing in a timely manner, in order to facilitate the dispatch without any interruptions to other operations. This in accordance with the operational manual.
- 5.4.3 The bidder shall provide adequate staff to ensure SLAs are met for the DTCs personalization unit.
- 5.4.4 DTC Quality Check error rate is 0.5% for a batch of 10,000 DTCs. Any batch exceeding this rate is charged with a penalty of LKR 10,000.00 per DTC.
- 5.4.5 The employer will request the DTCs (Phase 2) in batches of 1,000,000 (1 million) from the bidder. The bidder shall be able to successfully deliver the request amount within 1 month from the date of the employer making the request.
- 5.4.6 Penalty charged for any delay delivering DTCs is LKR 100,000.00 per day.

5.5 [Item 6 and 7] – NDI Hosting Infrastructure and Certificate Authority

5.5.1 Warranty Requirements

- 5.5.1.1 The warranty period shall be sixty months (60 months) comprehensive on-site bidder authorized warranty (Labor and Parts) with one to one backup in case workshop attention is required for all hardware components.
- 5.5.1.2 60 months comprehensive on-site warranty shall commence from the Acceptance of the solution by the Employer.
- 5.5.1.3 For purposes of the Warranty, “on-site” is the place(s) of final destination sites specified by the employer
- 5.5.1.4 For purposes of the Warranty, “on-site” means Bidder shall allocate adequate staff to visit the site to identify the problem and resolve the problem in coordination with employer
- 5.5.1.5 Annually One (1) dedicated preventive maintenance service shall be provided by the bidder during the period of warranty and submit completion report to employer.
- 5.5.1.6 Bidder must maintain spare parts stock for repairs and replacements for the duration of the warranty service period.
- 5.5.1.7 Bidder must bear all charges with regard to the supply of spare parts, labour, travel, per diem and accommodation to the bidder staff etc; during the period of warranty. Employer will NOT pay any additional expenditure for services rendered during the warranty period.
- 5.5.1.8 Bidder must adhere to the Warranty Support Service Level Agreements listed in the under SECTION 5 - Service Level Agreements

5.5.2 Service Level Agreement (SLA)

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

5.5.3 Objectives of Service Level Agreements

- 5.5.3.1 To create an environment conducive to a co-operative relationship between Employer, Bidder and Employer's representatives (government organizations) to ensure the effective support of all end users.
- 5.5.3.2 To document the responsibilities of all parties taking part in the Agreement.
- 5.5.3.3 To define the commencement of the agreement, its initial term and the provision for reviews.
- 5.5.3.4 To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.

- 5.5.3.5 To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
- 5.5.3.6 To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.
- 5.5.3.7 To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

5.5.4 SLA’s for Live Data Center and Certification Authority.

5.5.4.1 Warranty Support SLA

Incident Management / Resolution	Live Data Center
Response for Resolution	
Critical Incident Response	1 hr
Major Incident Response	2 hrs
High Incident Response	4 hrs
Time to Fix	
Critical Incident	4 hrs
Major Incident	8 hrs
High Incident	10 hrs

5.5.4.2 Warranty Support SLA 2

Severity Level	Description	Type of Issues
Critical (24x7)	Live site cannot function	Any kind of hardware/firmware component issue that leads complete live site outage.(FW cluster failure, Switch cluster failure..etc) Any kind of system level (Operating system, hypervisor, management.. etc) failure which leads complete live site outage.
Major (8:00 a.m. to 5:00 p.m.)	Live Site functions at degraded performance level	Any kind of hardware/firmware component issue that leads to degrade the 50% or lower performance of the site (Server failure, FW failure, switch

		failure..etc) Any kind of system level (Operating system, hypervisor, management.. etc) failure which leads 50% or lower performance level.
High (8:00 a.m. to 5:00 p.m.)	Live Site functions at degraded performance	Any kind hardware, firmware, system application level failure which won't affect the performance, but need to be rectify and restore to the working state. (Power supply failure, KVM failure, Management and monitoring system failure, etc)

5.5.5 Penalties

If problems are not corrected within the time limit specified (Response + Resolution time in Warranty support SLA 1), the bidder shall be entitled to a penalty payment as specified below for each hour that the Bidder fails to resolve the problem during the above SLA.

- 5.5.5.1 Critical : LKR 100,000/- per hour
- 5.5.5.2 Major : LKR 75,000/- per hour
- 5.5.5.3 High : LKR 50,000/- per hour

5.6 [Item 8] – Household Transfer Management (HTM) System

5.6.1 Introduction

The aim of this agreement is to provide a basis for close co-operation between the Employer and the Bidder for support and maintenance services to be provided by the Bidder, 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.

5.6.2 Objectives of Service Level Agreements

- 5.6.2.1 To create an environment conducive to a co-operative relationship between Employer, Bidder and Employer's representatives (government organizations) to ensure the effective support of all end users.
- 5.6.2.2 To document the responsibilities of all parties taking part in the Agreement.
- 5.6.2.3 To define the commencement of the agreement, its initial term and the provision for reviews.
- 5.6.2.4 To define in detail the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.
- 5.6.2.5 To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
- 5.6.2.6 To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.
- 5.6.2.7 To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

5.6.3 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.

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 Employer and Bidder. In the event of a discrepancy between actual and targeted service levels both Employer and Bidder are expected to identify and resolve the reason(s) for any discrepancies in close co-operation.

Service level monitoring will be performed by Employer. Reports will be produced as and when required and forwarded to the Bidder.

5.6.4 Support Levels

The bidder must provide support and maintenance services during Support Levels mentioned below;

Support Level 2 : Medium	
Component/ Service	Household Transfer Management (HTM) system
Support Hours	From 08:30 AM to 05:30 PM Monday to Friday (excluding public holidays)

5.6.4.1 SLA applicable during the services and maintenance period, applicable as the UAT certificate is issued: Support 2.

5.6.5 On-Call Services Requirements

Bidder must make at least one qualified personnel available to the Employer by telephone, email and issue tracking system for the reporting and resolution of non-conformities or other issues, defects or problems.

Dedicated telephone numbers, emails, tracking system shall be available for reporting issues.

Employer will nominate the personnel who are authorized to report non-conformities or other problems with the system. Reporting of non-conformities includes requests by the Employer to apply critical software updates or patches.

Table-1 shows the response priority assigned to faults according to the perceived importance of the reported situation and the required initial response times for the individual priority ratings. All times indicated represent response time during specified Support Levels.

The indicated response time represents the maximum delay between a fault /request being reported and a Bidder's representative contacting the Employer by telephone.

The purpose of this contact is to notify the Employer of the receipt of the fault /request and provide the Employer with details of the proposed action to be taken in respect of the particular fault /request.

Support Level	Business Critical		Non-Business Critical	
	Fatal	Impaired	Fatal	Impaired
High	60 minutes within Support Hours	90 minutes within Support Hours	90 minutes within Support Hours	120 minutes within Support Hours

Table-1: Response Priority

Note:

- Fatal - Total system inoperability
- Impaired - Partial system inoperability
- Business Critical - Unable to perform core business functions
- Non-Business Critical - Able to perform limited core business functions

Furthermore, time to resolve the Problem, is support level time, starting from the actual time of receiving the bidder notification. However if the notification is occurred outside the defined support level time, then time to resolve the Problem, is support level time, starting from as the next support level begins.

5.6.6 **Problem Resolution and Penalties**

If faults are not corrected within the time limits specified in the Table-2, the Employer will be entitled to a penalty payment for each hour that the Bidder fails to resolve the fault.

Support Level	Business Critical		Non-Business Critical	
	Fatal	Impaired	Fatal	Impaired
Medium	6 Hours LKR 50,000.00 per hour	10 Hours LKR 50,000.00 per hour	10 Hours LKR 50,000.00 per hour	15 Hours LKR 50,000.00 per hour

Table-2: Resolution Time and Penalties

5.7 General

Having understood the above warranty and Service levels, the bidder shall submit a detailed proposal in compliance with the above and indicating, among others, how the following are dealt with

- 5.7.1 Severity Levels
- 5.7.2 Severity Levels of Production Support Incidents
- 5.7.3 Scope of Support Engagements
- 5.7.4 Updates
- 5.7.5 Creating and Managing Support Incidents
- 5.7.6 Helpdesk
- 5.7.7 Phone Support
- 5.7.8 Conditions for Providing Support Services
- 5.7.9 Exclusions from Support Services
- 5.7.10 Changes to or Discontinuance of Support Services

INSPECTION COPY

6 Bill of Material (BOM)

ITEM	PROCUREING ITEMS	QUANTITY
1	ENROLMENT STATIONS	
	Notebook	1,783
	Latch cables	1,783
	Scanner	1,783
	POS Printer	1,783
	USB Hub	1,783
	Camera	1,783
	Fingerprint (10) Scanner	1,783
	Iris Scanner	1,783
	USB 1 finger scanner (Enrolment staff)	1,783
	PIN Printer	1,783
	Enrolment staff Table (*)	790
	Enrolment staff Chair (*)	790
	Citizen Chair (*)	790
	Extension cable (6 plugs)	1,783
	Power Cabling (13A)	1,783
2	Portable Unit	331
3	Centralized NDI solution	Item
4	Training of Enrolment Staff	1,900
5	Digital Transaction Cards (DTC) Personalization and Issuance	
	DTC Cards (Phase 1)	5,000
	DTC Cards (Phase 2)	14,000,000
	DTC Personalization units	35
	Notebook (Personalization unit)	35
	Notebook (QC unit)	35
	Notebook (Dispatch unit)	35
	Monitors	35
	Finger Print Reader	506
	USB Card Reader	506
6	Certificate Authority and Signature Signing and Authenticating Services Solution (High available)	Item
7	NDI Systems Infrastructure (HA, Active-Active)	Item
8	Household Transfer Management (HTM) system	Item

6.1.1 * A special arrangement has been made with concurrence of the Department of Registrar of Persons (DRP) to obtain the items which are already available

at the Divisional Secretariat locations. However, this number may vary due to the decisions coming from the National Steering Committee regarding obtaining the said items from DRP.

- 6.1.2 Below mentioned architecture and specifications are the minimum requirements and the bidders are to propose enhanced detail infrastructure diagram and specifications to be used.

6.1.2.1 Production Data Center (Per Site)

Item No	Item Name	Quantity (Minimum)
1	External Firewalls	2
2	Internal Firewalls	2
3	Ethernet Switches	2
4	SAN Switches	2
5	Application Servers	6
6	Database Servers	3
7	Management Servers	3
8	SAN	1
9	Backup Solution (On Site)	1

7 Specifications

7.1 [Item 1] - Enrolment Stations

7.1.1 Notebook

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Brand	Shall be internationally reputed brand (Specify)			
Model	(Specify)			
Country of Origin & Country of Manufacture /Assembly	(Specify)			
Year of manufacture	(Specify)			
Processor	Intel Core i5 6 th Generation			
Processor speed	2.3 GHz or better (Base Frequency)			
Chipset	Compatible (Specify)			
Cache	3 MB Cache or better			
Memory	4 GB DDR3 or better with a free slot			
Hard Disk	256 GB SATA MLC SSD			
Display	14 inch diagonal LED-backlit HD			
Resolution	WXGA			
Graphics	Integrated Graphics with min 512MB or more			
Optical Drive	DVD+RW Super Multi DL			
Audio	HD audio; Integrated stereo speakers; integrated digital microphone; Stereo headphone/line out; Stereo microphone/line in			
Webcam	Integrated 2 MP webcam or better			
Network	Ethernet (10/100/1000 NIC) or better			
Wireless	Built in 802.11 b/g/n and Bluetooth			
Card Reader	Integrated Media Card Reader			
Details of I/O (Input/output) ports	3 x USB 2.0 or better			
	1 external VGA port			
	1 HDMI			
	1 AC power			
	1 RJ-45			
Security	Laptop Lock Cable shall be provided			
	USB Thumb Reader device shall be provided			

Battery Life	Minimum up to 4 hours			
Keyboard	spill-resistant keyboard			
Weight	2.2Kg or lesser weight			
Carrying Case	Must provide with the Same Brand			
Operating System	Licensed Operating System which supports complete application stack.			
Productivity Software	As per the requirements, properly licensed applications to be installed.			
Manufacturer Authorization	Manufacturer authorization letter shall be provided			
Compliance	Standard compliance certificate to be provided from a suitably qualified third party authority.			
Product Experience	Notebooks shall be produced under the same brand for at least for last 10 years.			
Warranty	5 years comprehensive on-site manufacturer authorized warranty (labor, parts and other incidentals).			

7.1.2 Scanner (Legal)

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes/No	If “No” Bidder’s response	
Brand	(Specify)			
Model	(Specify)			
Country of Origin/ Manufacture	(Specify)			
Scanner type	Flatbed, ADF			
Digital sending standard features	Scan to folder, scan to email, scan to copy, scan to application			
Scan resolution, optical	Up to 1200 dpi			
Duty cycle (daily)	500 pages or better			
Bit depth	48-bit minimum			
Multifeed detection	Standard			
Automatic document feeder capacity	(Specify)			
Automatic document feeder scan speed	50 ppm (b&w, grey, colour, 200 dpi)			
Scan size (flatbed), maximum	Legal			
Scan size (ADF), maximum	Legal			

Scan size flatbed (minimum)	(Specify)			
Media types	Paper (plain, inkjet, photo), envelopes, cards (index, greeting)			
Media weight	(Specify)			
Scan file format	PDF (formatted Text and Graphics, normal with images, searchable image over text, MRC, PDF/A), TIFF (single page, multi-page, compressed), JPG, BMP, PNG, DOC, RTF, TXT, WPD, XLS, HTM, OPF, UNICODE, XML, XPS			
Control panel	2 quick start buttons (Scan, Copy), Cancel, Tools, Power save			
Operating humidity range	(Specify)			
Connectivity, standard	Hi-Speed USB 2.0 or better			
Minimum system requirements	Shall be compatible with Microsoft Windows Family Mac OS Ubuntu/ Linux			
Warranty	Manufactures Warranty for Five (05) years, inclusive of replacement of all defective parts free of charge.			
Product Experience	Scanners shall be produced under the same brand for at least for last 5 years.			
Compliance	Standard compliance certificate to be provided from a suitably qualified third party authority.			
Manufacturer Authorization	Manufacturer authorization letter shall be provided			

7.1.3 POS Printer

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Brand	(Specify)			
Model	(Specify)			
Country of Origin/ Manufacture	(Specify)			
Type	Desktop POS Printer			
Print Method	Thermal			
Print Speed	11.8" per second or better			
Connectivity Interface	USB 2.0 or better			
Paper Dimention	80 mm			
Paper Thickness	55 – 80 µm			
Auto cutter	Standard			

Barcode	UPC-A/E, CODE 39/93/128, EAN8/13, ITF, CODABAR 2D symbols: PDF417, QR-CODE, MaxiCode, Composite Symbology, GS1-128, GS1 DataBar Omnidirectional /Truncated/Limited/Expanded			
Data Buffer	4KB or better			
Accessories	Power Supply Unit			
	Divers			
	USB Cable			
OS Support	Windows Family Mac OS Ubuntu/ Linux			
Product Experience	PoS Printers shall be produced under the same brand for at least for last 5 years.			
Compliance	Standard compliance certificate to be provided from a suitably qualified third party authority.			
Warranty Manufacturer Authorization	5 Years comprehensive on-site Warranty Manufacturer authorization letter shall be provided			

7.1.4 USB Hub

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes/ No	If “No” Bidder’s response	
Brand	(Specify)			
Model	(Specify)			
Country of Origin/ Manufacture	(Specify)			
Number of Ports	07 or better			
USB interface	USB 2.0 or better			
Features	Plug and Play Built in cable management			
Data Transfer Rate	480 Mbps or better			
OS Support	Windows Family Mac OS Ubuntu/ Linux			
Warranty	5 Years comprehensive on-site Warranty			
Manufacturer Authorization	Manufacturer authorization letter shall be provided			

7.1.5 Dual Iris Scanner

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Brand	(Specify)			
Model	(Specify)			
Country of Origin/ Manufacture	(Specify)			
Type	Dual Iris Scanner			
Features	Automatic Dual Iris detection and capturing ISO compliant iris images utilizing multi wavelength IR illuminators Distance sensor and a tri-color LED position Indicator Eye safety standard (IEC 62471:2006-07), or specify RoHS FCC-Class A, IP54 ISO/IEC 19794-5/6			
SDK	Availability of SDK			
General	Export capability of biometric records to external systems in standard data formats.			
Interface	Standard USB 2.0			
Product Experience	Iris scanners shall be produced under the same brand for at least for last 5 years.			
Manufacturer Authorization	Manufacturer authorization letter shall be provided			
Compliance	Standard compliance certificate to be provided from a suitably qualified third party authority.			
Warranty	5 Years comprehensive on-site warranty			

7.1.6 Camera.

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Brand	(Specify)			
Model	(Specify)			
Country of Origin/ Manufacture	(Specify)			

Type	2D Face image capturing camera			
Sensor	5MP or higher			
Features	Ability to produce ISO/IEC 19794-5 (ICAO Standard) Integrated Flash for images capturing.			
Mounting	Tripod mount.			
Sensitivity	ISO 3200			
File Format	Common Biometric Exchange File Format (CBEFF), JPEG, JPEG2000			
Interface	Standard USB 2.0			
Product Experience	Cameras shall be produced under the same brand for at least for last 5 years.			
Manufacturer Authorization	Manufacturer authorization letter shall be provided			
Compliance	Standard compliance certificate to be provided from a suitably qualified third party authority.			
Warranty	5 Years comprehensive on-site warranty			

7.1.7 Finger Print Scanner (10 Fingers)

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Brand	(Specify)			
Model	(Specify)			
Country of Origin/ Manufacture	(Specify)			
Scan Area	132 x 130 mm			
Sensing Area	3.2” x 3.0”			
Roll Print Size	1.6” x 1.5”			
Image Resolution	500 dpi			
Standards	FBI IAFIS IQS CJIS-RS-0010 (V7) Appendix F compliance ANSI/NIST-ITL 1-2007ISO/IEC FCD 19794-4ANSI/NIST-ITL 1-2000ANSI/NIST-ITL 1-2000 Interpol Implementation			
Interface	USB 2.0			
Power Supply	12 V (adapter ~220 V, 50 Hz)			
Scanner Size (W x D x H)	(Specify)			
Scanner Weight	(Specify)			
Operating Systems	Windows, Linux			
Warranty	5 Years comprehensive on-site warranty			
Manufacturer	Manufacturer authorization letter shall			

Authorization	be provided			
Product Experience	Finger print scanners shall be produced under the same brand for at least for last 5 years.			
Compliance	Standard compliance certificate to be provided from a suitably qualified third party authority.			

7.1.8 Tables

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Specifications For Staff (Enrolment)	120x60x75 cm (LxWxH) shall be available 1 lockable drawer or better wood finish appearance easy cable entry/exit provisions			
Warranty	5 years comprehensive on-site warranty			

7.1.9 Chairs

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Specifications (Enrolment Staff)	Mid-back Shall be rotatable and height adjustable Arm rests Casters for easy movements			
Specifications (Citizen)	Low-back Shall be rotatable and height adjustable Casters for easy movements			
Warranty	5 years comprehensive on-site warranty			

7.2 [Item 2] - Portable Unit

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Brand	(Specify)			
Model	(Specify)			
Dual Iris/Face Camera	Automatic Dual Iris detection and capturing ISO compliant iris images utilizing dual frequency near infrared illuminators Distance sensor and a tri-color LED position Indicator Eye safety standard (IEC 62471:2006-07), RoHS FCC-Class A, IP54 ISO/IEC 19794-5/6 2D face capturing			
Laptop	Intel based laptop with required ports, drivers and enrollment/ authentication applications.			
Scanner	Flatbed Scanner			
Fingerprint Scanner	FBI Appendix F approved live scan device Supports collection of slaps and rolls 500ppi fingerprint images ANSI/NIST-ITL 1-2007ISO/IEC FCD 19794-4ANSI/NIST-ITL 1-2000ANSI/NIST-ITL 1-2000 Interpol Implementation			
Carrying case	Lockable, rugged carrying case			
Product Experience	Portable units shall be produced under the same brand for at least for last 5 years.			
Manufacturer Authorization	Manufacturer authorization letter shall be provided			
Compliance	Standard compliance certificate to be provided from a suitably qualified third party authority.			
Warranty	5-Year comprehensive warranty			

7.3 [Item 3] - Centralized NDI Software Solution

7.3.1 Following specifications are required for the centralized NDI solution for User Enrollment

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Product Name	(Specify)			
Licensing	2500 Enrolment Licenses			
Data Collection Fields	Name			
	Address			
	NIC			
	Finger Prints (10 Fingers)			
	Iris			
	Birth Certificate Info			
	Photo			
Features of Data Collection	Configurable to add more fields			
	Shall have tenant logins with biometric for users			
	Shall capture on client end, verify against existing data on database to avoid duplication within 5 seconds.			
	Shall support minimum 20 Million user records on Storage Database (Data Collection Fields specified above)			
	Customizable report generation			
Cash/Credit Card Collection	Receipt shall be able to be Printed			
	Shall accept credit/debit cards automated / manual entries			
Card & PIN Delivery	Advice of Dispatch to be printed			
	User Record updated after delivery of Card & PIN			
High Availability	Database Server			
	Application Server			

7.3.2 Following specifications are required for the centralized NDI solution for User matching Server Applications (biometric)

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Product Name	(Specify)			
Licensing	Unlimited Request from any Device			
Matching Criteria	National Identity Card Number			
	Card Unique ID			
	User Unique ID			
	Finger Prints (Any 10 Fingers)			
	IRIS Recognition			
	Face Recognition			
Speed of Matching (1,000 per second)	Minimum 1,000 Authentications per second with response time less than 1 second based on National Identity Card Number			
	Minimum 1,000 Authentications per second with response time less than 1 second based on Card Unique ID			
	Minimum 1,000 Authentications per second with response time less than 1 second based on User Unique ID			
	Minimum 1,000 Authentications per second with response time less than 1 second based on Finger Prints (Any 4 Fingers)			
	Minimum 1,000 Authentications per second with response time less than 1 second based on IRIS Recognition			
	Minimum 1,000 Authentications per second with response time less than 1 second based on Face Recognition			
Test Reports for Authentication Core Engine	Reliability testing results			
Software Development Kit (SDK) / APIs	Relevant APIs shall be provided			
High Availability Servers	Relevant all software components			

7.3.3 Search

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Criteria	All the text fields shall be searchable. Shall be full text based high speed search			

7.3.4 Finger Print Standards

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
1	BioAPI 2.0 (ISO/IEC 19784-1:2006)			
2	ISO/IEC 19794-2:2005 (Fingerprint Minutiae Data)			
3	ISO/IEC 19794-2:2011 (Finger Minutiae Data)			
4	ISO/IEC 19794-4:2005 (Finger Image Data)			
5	ISO/IEC 19794-4:2011 (Finger Image Data)			
6	ANSI/INCITS 378-2004 (Finger Minutiae Format for Data Interchange)			
7	ANSI/INCITS 378-2009 (Finger Minutiae Format for Data Interchange)			
8	ANSI/INCITS 381-2004 (Finger Image-Based Data Interchange Format)			
9	ANSI/INCITS 381-2009 (Finger Image-Based Data Interchange Format)			
10	ANSI/NIST-CSL 1-1993 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)			
11	ANSI/NIST-ITL 1a-1997 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)			
12	ANSI/NIST-ITL 1-2000 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)			
13	ANSI/NIST-ITL 1-2007 (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)			
14	ANSI/NIST-ITL 1a-2009			

7.3.5 Face Standards

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
1	BioAPI 2.0 (ISO/IEC 19784-1:2006)			
2	ISO/IEC 19794-5:2005 (Face Image Data)			
3	ISO/IEC 19794-5:2011 (Face Image Data)			
4	ANSI/INCITS 385-2004 (Face Recognition Format for Data Interchange)			
5	ANSI/NIST-CSL 1-1993 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)			
6	ANSI/NIST-ITL 1a-1997 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)			
7	ANSI/NIST-ITL 1-2000 (Data Format for the Interchange of Fingerprint, Facial, & SMT Information)			
8	ANSI/NIST-ITL 1-2007 (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)			
9	ANSI/NIST-ITL 1a-2009 (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information)			

7.3.6 IRIS Standards

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
1	BioAPI 2.0 (ISO/IEC 19784-1:2006) (Framework and Biometric Service Provider for iris identification engine)			
2	ISO/IEC 19794-6:2005 (Iris Image Data)			
3	ISO/IEC 19794-6:2011			
4	ANSI/INCITS 379-2004 (Iris Image Interchange Format)			

7.4 [Item 4] – Training Enrolment Staff

Item	Minimum Requirement	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
1	Training personnel shall be fluent at least one language from Sinhala or Tamil + English.			
2	Shall have a proper training plan and methodology to complete the enrolment staff training.			
3	Training curriculum shall be prepared and shall obtain prior approval before start training programs			
4	Shall assign most qualified personnel who have deep knowledge and training skills			
5	All training materials shall be available in English language.			
6	Each enrolment staff personnel shall have been given training minimum of 7 hours.			
7	Fully comply with “4.5 Training Enrolment Staff”, “4. Scope of Services” specified above			

7.5 [Item 5] - Digital Transaction Cards and Personalization

Supply, delivery, installation, commissioning, personalization and issuance of Digital Transaction Cards (DTC) and related equipment.

7.5.1 USB Card Reader

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes/ No	If “No” Bidder’s response	
Brand	(Specify)			
Model	(Specify)			
Country of Origin/ Manufacture	(Specify)			
Dimensions	70 mm (L) x 70 mm (W) x 115 mm (H) (Specify)			
Type	ISO7816 contact and ISO14443 contactless reader			
Interface	USB 2.0 or better			
Supply Voltage	Regulated 5 V DC			
Supply Current	Max. 50 mA (Specify)			
Operating Temperature	0-50 °C (Specify)			
CLK Frequency	4.8 MHz			
MTBF	500,000 hrs			
Smart Card Interface Support	ISO 7816 Class A, B and C (5 V, 3 V, 1.8 V)			
Compliance / Certifications	EN60950/IEC 60950, ISO7816, CE, FCC, VCCI, PC/SC, CCID, EMV 2000 Level 1, PBOC, RoHS 2, REACH, USB Full Speed			
	Microsoft WHQL			
Operating System Support	Windows			
	Linux			
	Mac OS			
Compliance	Standard compliance certificate to be provided from 3 rd party certification authority.			
Warranty	5 Years comprehensive on-site Warranty			
Manufacturer Authorization	Manufacturer authorization letter shall be provided			

7.5.2 Personalization Machine (Smart Card Printer)

Item	Minimum Specification /Requirement	Compliance		Reference (Section No and Page NOs)
		Yes/No	If “No” Bidder’s response	
1	Brand (Specify)			
2	Model (Specify)			
3	Country of origin/ Manufacture			
4	Manufacturer’s Year			
5	Personalization machine shall have an input hopper to stack smart cards of ID1 size as defined in ISO/IEC 7810 standard.			
6	Personalization machine shall have registration camera integrated in it.			
7	Personalization machine shall support chip encoding for contactless cards as per ISO/IEC 14443- 3 standard and contact cards as per ISO/IEC 7816-3 standard.			
8	Personalization machine shall support laser engraving of polycarbonate card at minimum 600dpi.			
9	Personalization machine shall support laser engraving of CLI feature in polycarbonate card.			
10	Personalization machine shall have an output hopper to stack personalized cards.			
11	Personalization machine shall have a reject bin to collect rejected cards during personalization process.			
12	Product Experience: Perso machines shall be produced under the same brand for at least for last 5 years.			
13	Manufacturer Authorization :Manufacturer authorization letter shall be provided			
14	Warranty: 5 Years comprehensive on-site Warranty			
15	Standard compliance certificate to be provided from 3 rd party certification authority.			


7.5.3 Smart Cards – (Phase 1 Digital Transaction Card (DTCs))

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
1	Brand (Specify)			
2	Country of Origin/ Manufacture			
3	Type : PVC Card			
4	White color			
5	Compatible with personalization machine (item 2)			
6	Graphic quality, glossy surface			

7.5.4 Smart Card – (Phase 2 Digital Transaction Card (DTCs))

7.5.4.1 Card body and Visual Personalization

Item	Minimum Specification /Requirement	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
	Brand (Specify)			
	Country of Origin (Specify)			
1	The card body shall be of ID1 size according to ISO/IEC 7810 standard and ISO/IEC14443 for cards with contactless chips in them.			
2	The smart card body is made of 100% polycarbonate multiple layers.			
3	The polycarbonate layers shall be fused under heat and pressure and are free of adhesives. Card body shall be designed both structurally and artistically such that it will be extremely difficult to imitate, reproduce, or manipulate in any manner. Forceful attempts to open the structure shall destroy the smart card.			
4	The polycarbonate layers shall not react under UV light (UV-dull)			
5	The card body design must consists of high security background, printed using direct tone offset technology and high resolution printing plates having minimum resolution of 4000dpi. Secure design shall be made of guilloches, micro text and other security elements. The design shall be created with a dedicated secure printing software.			
6	The secure design must include Rainbow printing.			
7	Micro text shall be part of background artwork of the card body with a character size not be more than 300µm.			
8	Micro text which is part of background shall also implement deliberate errors.			
9	The card body must include a specific true-colour UV image with high brilliance, resolution and high colour reproduction. The image shall become visible under a UV light source at 365nm.			

10	The card body must contain positive and negative surface embossing. That is embossing that goes inside the structure of the document and embossing that protrudes above the surface of the document. Positive and negative surface embossing on the card body shall implement micro texts with deliberate error			
11	The card body must implement CLI/MLI feature, it can be personalized with 2 different pieces of information, which are visible clearly from 2 different angles. The CLI/MLI feature in the card body shall be in shape of Sri Lanka government emblem outline. (A high resolution standard digital copy would be made available to the bidder)			
				
12	The smart card manufacturer must offer card body that contains elements with optical effects, light reflection, kinematic effects, high quality latent image effect and animated/moving effects which are spread all over the card body.			
13	The card body shall be compliant with 10 years lifespan.			
14	It shall not be possible to separate the different layers of the card body.			
15	The card body must contain laser-engraved markings protecting against delamination, tampering and cutting attempts.			
16	Demographic data and photo of card holder shall be personalized through laser engraving giving high resolution black and white personalization of more than 600dpi. This 600dpi resolution for personalization is chosen to have balance between high quality laser engraving and optimum throughput from personalization machine.			
17	Personalization data elements on card shall be personalized in a way they protect secure artwork. Some of data shall be personalized with tactile effect while rest of data shall be personalized below surface layer of the card body.			
18	The smart card manufacturer must submit their samples containing each of requested features along with tender answer by the bidder.			
19	Smart card for this project shall manufactured in a			

	manufacturing site which has valid ISO 9001, ISO 14001 & ISO 27001, ISO 14298 or CWA 14641 certificates.			
20	Smart card manufacturer must have a backup polycarbonate site to ensure business continuity and disaster recovery. The backup site shall also have above certificates.			
21	Smart card manufacturer shall provide ISO/IEC 10373 standard based test report on their sample polycarbonate cards from an independent internationally recognized 3rd party laboratory.			
22	Cards must be cryptographically secure during the transporting and only the KM can open the card for writing.			

7.5.4.2 Chip and operating system specification

Item	Minimum Specification /Requirement	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
1	The smart card manufacturer must master the full smart card value chain. The smart card manufacturer must have in house smart card operating system development and cryptographic library development.			
2	Smart card shall be microprocessor based IC card with contactless interface compliant to ISO /IEC 14443-3 standard.			
3	Chip shall work with nominal supply voltage 3V.			
4	Chip shall have min 10 years data retention.			
5	Chip shall have min 500,000 read/write cycles.			
6	Chip shall have operating ambient temperature range –25 Degree Celsius to +55 Degree Celsius.			
7	Chip shall be common criteria EAL5+ certified.			
8	Card OS shall comply with Global Platform 2.1.1 and Java card 2.2.2 or later versions.			
9	Card OS shall support multiple application to be loaded on the card and provide dedicated cryptographic services for respective applications.			
10	Card OS shall support PACE V2 for privacy protection.			
11	Card shall support communication protocol T=CL Type A or Type B.			
12	Card shall give minimum 64 KB of memory for user data.			

13	Card shall be common criteria EAL5+ certified with Java card System Protection Profile			
14	Card shall have preloaded applications for <ul style="list-style-type: none"> a. Secure storing of demographic data and digital keys, certificate. This application shall also support post issuance update of demographic data and digital keys, certificate. The application shall support all the necessary Public-Key features including signing, authentication Etc. b. Secure storing of fingerprint data of card holder inside the chip memory. This application shall be able to do fingerprint authentication using match on card mechanism. c. The card shall have provision to load multiple application if required. 			
APPLICATION FOR SECURE STORING OF DEMOGRAPHIC DATA, DIGITAL CERTIFICATE AND SUPPORT PKI				
15	This application shall comply with ISO/IEC 7816 – 4, 5, 6, 8, 9, 15.			
16	Application shall be used to securely store all the demographic information of card holder			
17	Application shall support PKCS #1, PKCS#15 and compliant with PKCS#11.			
18	Application shall support various cryptographic functions as below 3DES (ECB, CBC). RSA 2048 bits or more Digital Signature 2048 bits or more SHA up to 256 bits On-Board-Key-Generation			
MATCH ON CARD APPLICATION				
19	Card shall have Match on card application for fingerprint storage and authentication. The original fingerprint template stored shall never go out of the smart card.			
20	Match on card application shall support ISO/IEC 19794-2 finger minutiae compact-size card formats.			
21	Match on card application shall support fingerprint authentication as defined in ISO/IEC 7816-11			
22	During fingerprint authentication the matcher in the smart card shall take the query fingerprint template as input and match it with the original fingerprint template inside the card. The result of matching coming out of card shall be only final matching decision.			
23	Match on card algorithm used shall have undergone successful evaluation under MINEX II.			

7.5.4.3 Personalization System

Item	Minimum Specification /Requirement	Compliance		Reference (Section No and Page NOs)
		Yes/No	If “No” Bidder’s response	
	Brand/ Model (Specify)			
GENERIC REQUIREMENTS				
1	The personalization system shall be flexible to enable easy updating in the future.			
2	The personalization system shall be constructed of separate modules of which each of them handles their own separate tasks.			
3	The personalization software shall be machine independent and it is required that the personalization software supplier (bidder) already has prior experience of using personalization machinery from several machine suppliers.			
4	The personalization software shall be ready for connection with any Global Platform, Java card / MULTOS smart card management system.			
5	The personalization software must be able to be installed to any standard, commercial Hardware			
6	The personalization platform shall be able to deploy in deferent scheme: centralized, decentralized or both scheme.			
7	Graphical User Interface(GUI) shall be easy to use and it shall provide a simple interface for managing the personalization process such as, production batch generation, rejection , re-work of the products, executing prioritization of orders, executing /sending queries to the data system etc.			
8	Secure PIN printing			
SYSTEM FOR PRODUCTION MANAGEMENT				
8	The production management system shall be a web application accessible from a web browser.			
9	The production management system shall provide a mean to manually make a batch of cards.			
10	The production management system shall also provide a mean to automatically make a batch using smart cards attributes like card type, shipment date and delivery point etc.			
11	The production management system shall be able to implement priority levels.			
12	The production management system shall allow to define a batch size and this size shall be configurable.			
13	The production management system shall interface with a relational database to store information.			

14	The production management system shall generate a production status for every batch generated.			
15	The production management system shall be able to take several types of request format: XML, Binary, text, TLV.			
16	The production management system shall integrate the white list coming from the card manufacturer.			
17	The production management system shall be able to manage smart card inventories.			
18	The production management system shall provide search functions to get access to the history of requests, batches and documents.			
19	The production management system shall notify the issuing request system if the request has been personalized or not and if the request is OK or NOK after quality check. For each NOTOK case a ERROR code shall be returned. These error messages shall be standardized to guarantee efficient support and troubleshooting.			
20	The production management system shall generate a production follow up listing mentioning all the smart cards contained for every batch to be personalized. The production management system shall also generate a delivery sheet that will contain the list of smart cards to be shipped to a delivery point.			
21	The production management system shall be able to generate any other report based on the information's stored in the production management database.			
22	The production management system shall support customization of the report template using report tools.			
23	The production management system shall support report export in PDF format or EXCEL format.			
24	The production management system shall support report printing.			
25	The production management system shall communicate using web service with other software components hosted in the same secured area.			
26	The production management system shall communicate using secure web service (HTTPS) with other software components hosted in the external world.			
27	The production management system shall ensure that the issuance request is coming from an authorized external system			
28	The production management system shall support mutual authentication scheme to authenticate with external systems.			
29	The production management system shall provide logging of each personalization. Every log shall contain information about the tasks executed, the operator who did the execution and the execution time.			
30	The production management system shall archive the log files.			
31	The production management system shall implement a purge mechanism. The purge shall delete production data files using a configurable retention period.			

32	The production management system shall give access to the log files only to the auditor's role who have the right to access log files.			
33	The production management system shall implement user and password authentication mechanism to get access to the system based on LDAP.			
34	The production management system shall implement at least three different roles: operator, administrator and auditor			
35	The production management system shall be able to implement specific rights configured for every role.			
36	The log files and production files shall be signed to ensure the data integrity.			
37	The sensitive data's in the production file shall be encrypted to ensure the data confidentiality.			
38	External system shall be authenticated to communicate with the production management system.			
39	The platform shall provide production dashboard to ease the management of the production.			
SYSTEM FOR DATA PREPARATION				
40	The personalization solution shall contain a system to prepare data for graphical and electrical (chip) personalization from the database			
41	The system for data preparation shall be able to receive orders in any format (e.g. XML) format and the response files shall be made according to the needs of the employer. Furthermore, the system shall provide an easy-to-use graphical user interface for defining and maintaining configurations.			
42	The data preparation system shall be modular and implement a data processing plug-in that must be easily integrated for every application to be personalized electrically in the card.			
SYSTEM FOR GRAPHICAL AND ELECTRICAL PERSONALIZATION				
43	A separate system shall be implemented to be in charge of the overall personalization process including electrical and graphical personalization.			
44	The system shall support contact personalization as per ISO/IEC 7816-3 standard (T=0, T=1 communication methods) and contactless personalization as per ISO/IEC 14443- 3 standard (Type A or Type B).			
45	The system shall support contact and contactless chips personalized either in simultaneous step or in different step during personalization.			
46	The system shall support scripting language for chip personalization.			
47	The system shall support identification of chip based on chip serial number and OS version, visual characters e.g. printed barcode or machine readable zone(MRZ) etc.			
48	The system shall support batch or on demand modes.			
49	The system shall support data fetch from database.			

50	The system shall support decryption of encrypted input			
51	The system shall support interface to key management system (KMS)			
52	The system shall provide status information about electrical personalization to the operator. Operators shall be able to follow the electrical personalization process from the GUI.			
53	The system shall support both front and back side personalization.			
54	The system shall support physical security features personalization like CLI, micro texts, laser engraving etc.			
55	The system shall support personalization of required text fields, images, QR code and MRZ lines.			
CARD KEY MANAGEMENT (KMS)				
56	A key management system shall be implemented to provide the transport/master key management and cryptographic functions necessary to prepare and store the confidential data (secret, diversified keys and certificates) for the personalization of products.			
57	The key management system shall implement following modules <ul style="list-style-type: none"> a. A License manager to securely activate the KMS features b. A Key administration module c. A Server module d. On card key generation e. CSR generation and export 			
58	The database for Key storage			
59	The system shall be scalable <ul style="list-style-type: none"> a. One HSM on one system b. Multiple HSMs on one system with load balancing c. Multiple HSMs on several KMS systems with load balancing and failover capability. 			
60	The system shall never store DTC keys generated for citizens.			
61	The system shall implement a trusted path mechanism to communicate with NDI CA.			
62	The system access control shall be role-based.			
63	The system shall support SSL/HTTPS standard protocol for secure communication with its clients.			
64	The system shall manage integrity control for keys and other confidential data.			
65	The system shall have load balancing features in order to have a high level of performance.			
66	The system shall support offline and online RSA key generation, certificate request.			
67	The system shall manage the key lifecycle management and obsolescence management.			
SYSTEM FOR QUALITY CONTROL				
68	A quality control system shall be provided to perform			

	electrical and visual verification of the personalized ID document against the order data.			
69	This system is a standalone system running on a dedicated workstation.			
70	The system for quality control shall contain an easy-to-use graphical user interface.			
71	The quality control system shall contain the following features. <ul style="list-style-type: none"> a. Visual verification b. Electrical verification c. Product identification 			
72	The quality control system shall contain capturing and storing reference images of product layout for comparison purpose.			
73	Visual security elements against reference product stored in the data base.			
74	The quality control system shall support reading of contact cards as per ISO/IEC 7816-3 standard (T=0, T=1 communication methods) and contactless cards as per ISO/IEC 14443- 3 standard (Type A or Type B).			
75	The quality control system shall show electrical data to the operator in the GUI.			
76	The quality control checking shall be manual.			
77	The system for quality control shall support product identification by sticker e.g. QR code or MRZ, identification information stored in the chip e.g. chip's serial number.			
78	Product Experience: Personalization systems shall be produced under the same brand for at least for last 5 years.			
79	Manufacturer Authorization: Manufacturer authorization letter shall be provided.			
80	Warranty: 5 Years comprehensive on-site Warranty			
81	Standard compliance certificate to be provided from 3 rd party certification authority.			

7.6 [Item 6] - NDI hosting infrastructure

7.6.1 Per data center

Item	Minimum Specification / Requirement	Compliance		Reference (Section No and Page NOs)
		Yes/ No	If “NO”, Bidder’s Offer	
	<ol style="list-style-type: none"> 1) For all active equipment in the hosting infrastructure, specify the brand, model, country of origin and manufacturing year. 2) Specific equipment shall be produced under the same brand for at least for last 10 years. 3) Manufacturer authorization letter shall be provided. 4) 5 Years comprehensive on-site Warranty. 			
Application & Management Servers	Dual Intel® Xeon® Processor E5-2600 v3 product family QPI 9.6 GT/s or more 12 cores or more, 30MB cache/processor DDR4 DIMM slots Minimum 128GB per server 2 x 3.5” / 2.5" fixed 450GB,15k SAS Hard Disks (RAID1) RAID 0, 1, 5, 10 Network Interface - Minimum dual-port 10GbE Base-T / dual-port 10GbE SFP+ IPMI based remote management console access. Support Hypervisors - Citrix® XenServer® VMware vSphere® ESXi, KVM, QEMU <u>Special Notes</u> All Management Servers(3Nos) to be connected to SAN (8G FC) with redundancy.			
Database Servers	Dual Intel® Xeon® Processor E5-2600 v3 product family with QPI up to 9.6 GT/s Up to12 cores, 30MB cache/processor DDR4 DIMM slots Minimum 128GB per server 2 x 3.5” / 2.5" fixed 450GB,15k SAS Hard Disks (RAID1)+ 3 x 3.5” / 2.5" 2TB SATA Hard Disks (RAID5)			

	<p>RAID 0, 1, 5, 10 Network Interface - Minimum dual-port 10GbE Base-T / dual-port 10GbE SFP+ Fabric HBA: 8Gbps FC HBAs IPMI based remote management console access. Support Hypervisors - Citrix® XenServer® VMware vSphere® ESXi, KVM, QEMU <u>Special Notes</u> All Servers (3Nos) to be connected to SAN (8G FC) with redundancy.</p>			
External/ Internal Firewalls	<p>High Availability (Active-Active) Identity based access and filtering (Layer 8) Application Filtering (Layer 7 NGFW) Intrusion Prevention System Web Application Level Firewall(WAF) Spoofing and DoS/DDoS prevention APT Prevention Policy based Bandwidth Management IPv4/IPv6 Dual stack support (Policy, IPS, WAF) NAT Support Static,OSPF, BGP Routing Support of port trunking and 16+ VLANs Multiple security zones. Regular signature updates. 1M Concurrent sessions WAF Throughput 1.5Gbps Upto 2Gbps IPS Throughput Up to 2,000 No. of IPSec Tunnels Configurable Internal/DMZ/WAN Ports 8 x 1GbE Ports SSHv2, Web, SNMPv2/3 Management. Realtime and historical monitoring and syslog support. Log view (IPS,WAF,Events) and Reporting. CE, FCC Compliance</p>			
SAN	<p>Dual Active-Active Storage Controllers and upgraded to the latest firmware level 8 x 8 Gb FC Ports or higher on each controller. 10/100Gbps FCoE/ iSCSI Host Ports or higher on each controller FC, FCoE, iSCSI Support within the same array Dual 6Gbps SAS Buses /FC-ALs Automatic disk rebuild and Automatic disk failover</p>			

	<p>Minimum 16GB Cache on Each Storage Controller or higher. Cache Upgradability 48GB or higher Ability to use Flash/SSD to improve the cache. Supported RAID Levels 0/1/5/6 Automatic storage tiering support. Minimum 100TB effective capacity (RAID6) with 8+2 RAID6 pools and 2TB SATA + 1TB(4+1 RAID5) SSD pool to improve IOPS + 2 x 2TB Spares. Support SAS, NL-SAS, Solid State/Flash Drives. Up to 1024 Maximum hosts supported Maximum LUN size 128TB Number of LUN 1024 or more Ability to take Snapshots / Clones Continuous Data Replication (Synchronous) to the SAN at DC2. Scalability upto 200 Disks.</p>			
SAN Switches	<p>8Gbps FC Fully redundant. Support for ISL and Link Aggregation. Secure Management Access</p>			
Rack Switches	<p>L2, L3 Support Full IPv6 Support in Hardware Redundancy 4096 VLANs, ACL's, Spanning tree and IEEE standards / protocols support Switch management - SNMP v2 Support, CLI-based management console, SSH v2 Support, Software Backup/Restore method Ethernet Ports - 10Gbps ports Stacked or ISLed Switches. MC-LAG/vPC/ IEEE 802.1aq Support and configured to each server. Secure Management Access.</p>			
Backup Solution.	<p>Inline Deduplicated D2D Backup Solution. 100TB Daily backup set with 3 Months Retention. Backup clients for hypervisors for VM backups. Backup server shall support parallel backup jobs to achieve 10TB/hr CBT(Change Block Tracking) based incremental backups. NFS and VTL Access method Direct SAN backups (VTL).</p>			

	2 x 10GbE and 2 x 8G FC Connectivity. 10TB/hr Throughput Replication over Ethernet to the Other site.			
Hypervisor	Each server shall be virtualized with Citrix XenServer, KVM, VMware vSphere®, ESXi, QEMU			
System Monitoring	SNMP and Agent based monitoring Email and SMS alerting Web front end. Support Network elements and servers.			
Rack	42U Rack with 16-Port PS/2 - USB KVM Switches with LCD monitor Same brand of the servers. Support dual power supply.			

INSPECTION COPY

7.7 [Item 7] - NDI Certification Service Provider (Certification Authority) and Services

Item	Minimum Specification	Compliance		Reference (Section No and Page NOs)
		Yes /No	If “No” Bidder’s response	
Product Name	(Specify)			
Licensing	Unlimited Certificates			
Hardware (Specify)	Servers			
	Ethernet Switches			
	Firewalls			
	UPS/Racks			
	HSMs(FIPS 140-2 level 3 Compliant)			
Server Room	Server Room Preparation (Location will be provided by the Employer) and Access control			
High Availability	Hardware infrastructure shall be highly available with no single point of failure.			
Application Modules	Signing Service, Verification Service Evidence Service			
	CA, RA, XKMS, OCSP/CRL, Secure Time Stamping Service modules.			
	Logging, Reporting, Archiving			
Client SDK	Shall be Available			
Backup Site	Backup Site shall be located at Production SiteII			
Replication and Backup	Live data shall synchronously replicated to backup site and Backups/Archives shall be maintained.			
Compliance	Processes, preparations and application stack shall be fully complied with WebTrust 2.0 or latest and shall get WebTrust seal from CPA Canada			
Product Experience	Certification authorities shall be produced under the same product name for at least for last 5 years.			
Manufacture Authorization	Manufacturer authorization letter shall be provided			
Warranty	5- Year comprehensive onsite warranty			

Description	Bidders Compliance	Reference (Section No and Page NOs)
7.8 [Item 8] – Household Transfer Management (HTM) system		
<p>7.8.1 Technical Qualification of the firm</p> <p>7.8.2 Experience of the firm with projects of similar nature;</p> <p>7.8.2.1 Submit case studies (if any) explaining your past project (a) implementation, (b) security consideration (c) deployment and (d) support and maintenance experiences related to the above software and deployment setup.</p> <p>7.8.2.2 Elaborate how you ensured the enterprise interoperability aspects. How APIs were integrated or developed in a typical SOA based environment with REST based integrations along with SOA security.</p> <p>7.8.2.3 Describe the usage of the middle-ware elaborating the SOA concepts and enterprise software architecture best practices used.</p> <p>7.8.2.4 Explain how the enterprise integration was handled and best practices used.</p> <p>7.8.2.5 Describe the usage of the Business Rules Management System (BRMS) elaborating the Business Rules Engine (BRE) used.</p> <p>7.8.2.6 How responsive UI templates were designed and implemented in order to facilitate different devices such as web and mobile.</p> <p>7.8.2.7 Elaborate the performance considerations in aforementioned projects. Elaborate how you ensured high availability and load balancing, considering application level failures in cloud environment.</p> <p>7.8.2.8 Elaborate use of any monitoring tools for maintainability.</p> <p>7.8.2.9 Brief explanation of degree of in-house SQA standards and procedures.</p> <p>7.8.2.10 Elaborate support and maintenance experiences related to the above software.</p>		

<p>7.8.2.11 The bidder shall be having a competent team of key professional who is capable of undertaking the design, delivery and operations of this solution. Their curriculum vitae shall demonstrate adequate knowledge and experience to undertake the assignment.</p> <p>7.8.2.12 The bidder shall propose the team structure.</p> <p>7.8.2.13 The bidder shall indicate their work allocation including onsite/offsite allocation</p> <p>7.8.2.14 The bidder shall elaborate any scope which they consider as out of their scope.</p>		
--	--	--

INSPECTION COPY

8 Facilities and services provided by the Employer

8.1 Key Activities

8.1.1	Establishment of National Data Facilitation (NDF) Centers	NDF Centers shall be established at District and Divisional Secretariat (DS) levels by the employer. Enrolments are carried out at NDF locations and will also function as a coordination point for mobile data collection initiatives.
8.1.2	Establishment NDI data verification centers	The employer will carry out first level verification of captured data and other artifacts at the NDI data verification centers. This center will be established in Colombo.
8.1.3	Enrolment and Management staff at NDF centers	The employer will recruit enrolment and management staff located at NDF centers and NDI verification centers from the government or private sector.
8.1.4	Equipment for NDI verification centers and management staff at NDF centers and	The employer will procure ICT equipment for the staff located at NDI verification centers. Further, employer will procure ICT equipment required for the management staff at NDF centers.
8.1.5	Improvements to the stakeholder systems	The employer will procure service providers to carry out improvements to the systems at stakeholder organizations associated with beneficiary programs. Service providers shall be procured via another separate tender.
8.1.6	Connectivity	NDF, NDI and enrollment centers connected via secure LGN connectivity.
8.1.7	Data Centers	Locations for data centers for live sites will be provided. Locations for NDI CA will be provided. All data center preparations, secure access and standards has to be implemented by the bidder.
8.1.8	National Payment Platform (NPP)	The NPP implemented in by the employer in collaboration with stakeholder organizations such as the Ministry of Finance, Central Bank of Sri Lanka and Financial Institutions, shall be made available by the employer for integrations with the HTM and other systems.

8.2 NDF Centers (Proposed)

Following are proposed NDF center designs and layouts

8.2.1 Proposed layout design of an enrolment station/desk

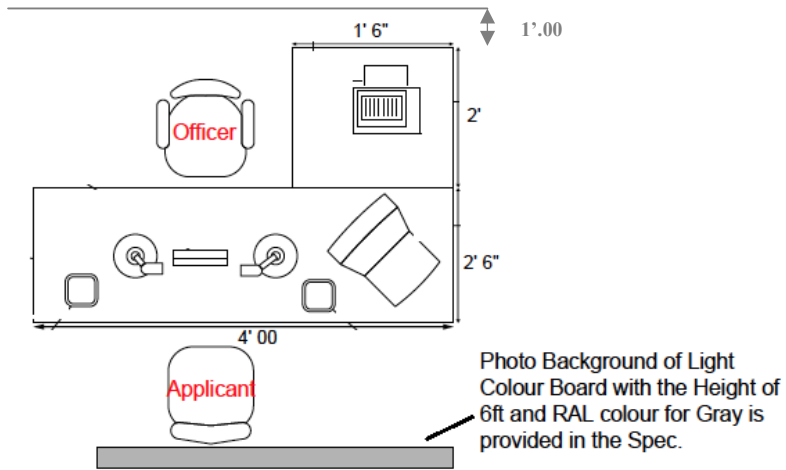


Figure 12: Proposed enrolment station / desk

8.2.2 Proposed layout design of a Manager /Supervisor station /desk

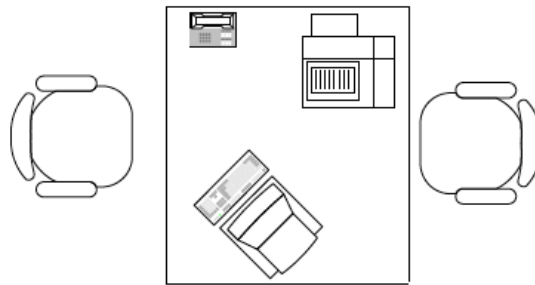


Figure 13: Proposed Manager /Supervisor station / desk

8.2.3 Proposed layout between stations/desks

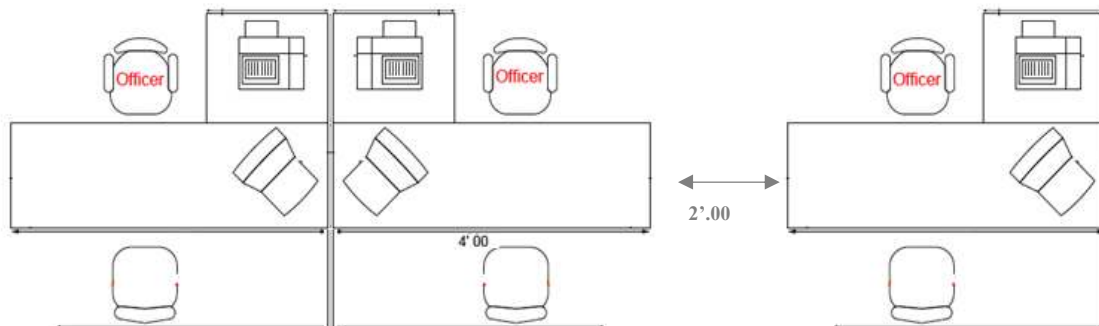


Figure 14: Layout between stations / desks

8.2.4 NDF center proposed layout at DS locations

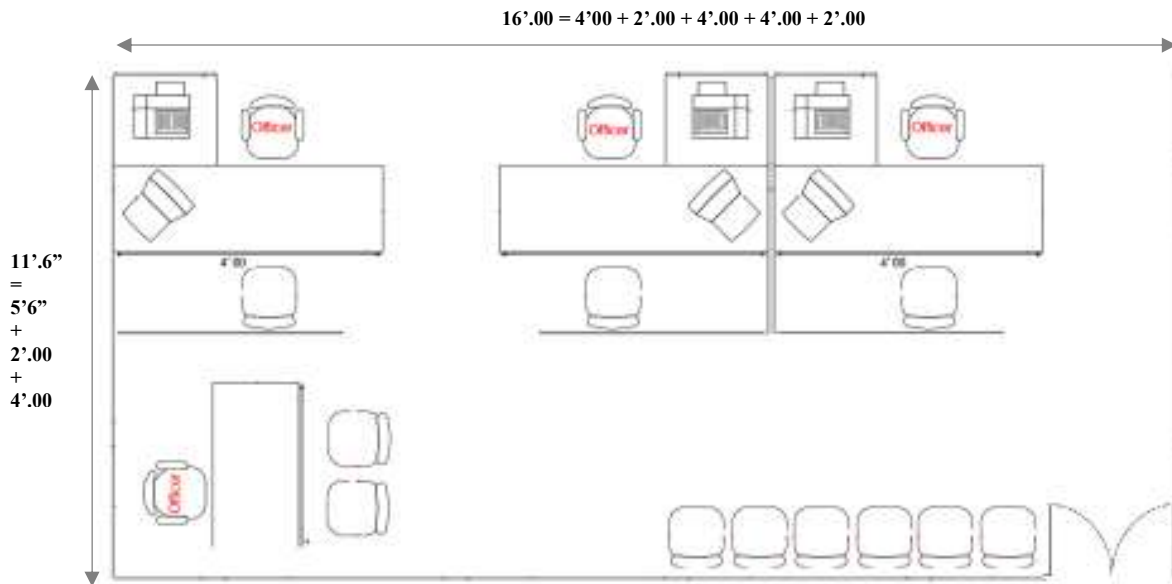


Figure 15: Proposed DS NDI center layout

8.2.5 NDF District Center proposed layout

8.2.5.1 The District NDF center shall consist of following units.

- 8.2.5.1.1 Ticket issuing counter (Queue no issuing counter)
- 8.2.5.1.2 Citizens waiting area
- 8.2.5.1.3 Enrolment stations/ desks
- 8.2.5.1.4 Supervisor stations/ desks
- 8.2.5.1.5 Manager stations
- 8.2.5.1.6 DTCs personalization unit.
- 8.2.5.1.7 DTCs issuing counter
- 8.2.5.1.8 Cafeteria for staff
- 8.2.5.1.9 Rest room

8.2.5.2 The proposal layout may vary depending on the structure of the venue, NDF center type and what has been proposed by the bidder.

8.2.5.3 However it is important for the bidder to specify a layout which will facilitate adequate space for all parties concerned (relevant people associated with above units) and obtain approval from the Employer.

ADP

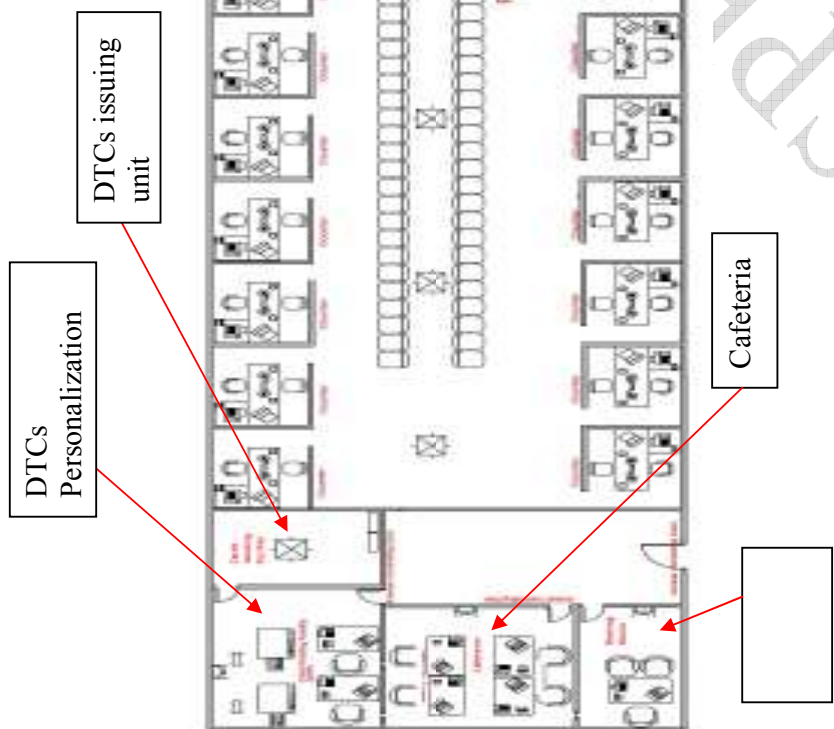


Figure 16: Proposed District NDF center layout.

INSPIRE

- 8.2.6 The Employer will provide the NDF Centers depending of the center type in a timely manner.
- 8.2.7 The Employer will ensure secure connectivity to the enrolment centers.
- 8.2.8 The Employer will provide adequate security for the NDF Centers.
- 8.2.9 The Employer will ensure proper awareness is done to ensure continued interest from citizens for enrolment.
- 8.2.10 The Employer will provide secure storage place for the portable devices.

8.3 Training of enrolment staff

- 8.3.1 The Employer will ensure the trainees (enrolment staff and other nominated people) are made available for the training in a timely manner, as agreed with the bidder.
- 8.3.2 The Employer will maximize the quality of training through a continuous mentoring and monitoring program defined and supervised by the employer.

8.4 Digital Transaction Cards (DTC) and Personalization

- 8.4.1 The Employer will ensure adequate support staff such as for staff for verification and translation units are employed to ensure smooth operation of DTCs personalization by the bidder.
For those DTCs which are to be issued to citizens via the DS NDF centers, the Employer will facilitate the distribution / transportation of those DTCs to respective NDF DS centers.

8.5 NDI Hosting Infrastructure

- 8.5.1 The Employer will provide an ICT infrastructure facility to host the entire system with highly available and high performance hardware.
- 8.5.2 Front-end application –Enrolment software
- 8.5.3 Front-end application – Authentication software
- 8.5.4 Backend solution for Enrolment management software
- 8.5.5 Database which store enrolment biometric and other personal identification data
- 8.5.6 Data center faculties for the LIVE I and LIVE II sites.
- 8.5.7 Internet and LGN Connectivity for both sites.

9 Locations

9.1 The Employer will setup NDF data collection centers throughout the country.

- NDF center at each district – 29 + centers
- NDF center at each DS – 331 centers

The exact site/ locations list will be circulated among the successful bidders.

9.2 NDF District Centers

No	District	No	District
1	Colombo	13	Moneragala
2	Gampaha	14	Anuradhapura
3	Kalutara	15	Polonnaruwa
4	Galle	16	Kurunegala
5	Matara	17	Puttalam
6	Hambantota	18	Ampara
7	Matale	19	Batticaloa
8	Kandy	20	Trincomalee
9	Nuwara Eliya	21	Vavuniya
10	Kegalle	22	Mannar
11	Ratnapura	23	Mullaitivu
12	Badulla	24	Kilinochchi
		25	Jaffna

9.3 NDF DS Centers

COLOMBO - 13 DSs

1	Divisional Secretariat, Colombo
2	Divisional Secretariat, Dehiwala
3	Divisional Secretariat, Seethawaka
4	Divisional Secretariat, Homagama
5	Divisional Secretariat, Kaduwela
6	Divisional Secretariat, Kesbewa
7	Divisional Secretariat, Kolonnawa
8	Divisional Secretariat, Maharagama
9	Divisional Secretariat, Moratuwa
10	Divisional Secretariat, Padukka
11	Divisional Secretariat, Ratmalana
12	Divisional Secretariat, Sri Jayawardhanapura Kotte
13	Divisional Secretariat, Thimbirigasyaya

GAMPAHA- 13 DS's

MONARAGALA - 11 DSs

167	Divisional Secretariat, Badalkumbura
168	Divisional Secretariat, Bibile
169	Divisional Secretariat, Buttala
170	Divisional Secretariat, Katharagama
171	Divisional Secretariat, Madulla
172	Divisional Secretariat, Medagama
173	Divisional Secretariat, Moneragala
174	Divisional Secretariat, Sevanagala
175	Divisional Secretariat, Siyambalanduwa
176	Divisional Secretariat, Thanamalvila
177	Divisional Secretariat, Wellawaya

ANURADHAPURA - 22 DSs

178	Divisional Secretariat, Padaviya
179	Divisional Secretariat, Kebithigollewa

14	Divisional Secretariat, Attanagalla	180	Divisional Secretariat, Medawachchiya
15	Divisional Secretariat, Biyagama	181	Divisional Secretariat, Mahavilachchiya Divisional Secretariat, Nuwaragam Palatha Central
16	Divisional Secretariat, Divulapitiya	182	Divisional Secretariat, Rambewa
17	Divisional Secretariat, Dompe	183	Divisional Secretariat, Kahatagasdigiya
18	Divisional Secretariat, Gampaha	184	Divisional Secretariat, Horowpothana
19	Divisional Secretariat, Ja-Ela	185	Divisional Secretariat, Galenbindunuwewa
20	Divisional Secretariat, Katana	186	Divisional Secretariat, Mihinthale Divisional Secretariat, Nuwaragam Palatha East
21	Divisional Secretariat, Kelaniya	187	Divisional Secretariat, Nachchadooda
22	Divisional Secretariat, Mahara	188	Divisional Secretariat, Nochchiyagama
23	Divisional Secretariat, Minuwangoda	189	Divisional Secretariat, Rajanganaya
24	Divisional Secretariat, Mirigama	190	Divisional Secretariat, Thambuttegama
25	Divisional Secretariat, Negambo	191	Divisional Secretariat, Thalawa
26	Divisional Secretariat, Wattala	192	Divisional Secretariat, Tirappane
	KALUTARA- 14 DSs	193	Divisional Secretariat, Kekirawa
27	Divisional Secretariat, Agalawatta Divisional Secretariat, Baduraliya (Palinda Nuwara)	194	Divisional Secretariat, Palugaswewa
28	Divisional Secretariat, Bandaragama	195	Divisional Secretariat, Ipalogama
29	Divisional Secretariat, Beruwala	196	Divisional Secretariat, Galnewa
30	Divisional Secretariat, Bulathsinhala	197	Divisional Secretariat, Palagala
31	Divisional Secretariat, Dodangoda	198	
32	Divisional Secretariat, Horana	199	POLONNARUWA - 07 DSs
33	Divisional Secretariat, Ingiriya	200	Divisional Secretariat, Elahera
34	Divisional Secretariat, Kalutara	201	Divisional Secretariat, Hingurakgoda
35	Divisional Secretariat, Madurawala	202	Divisional Secretariat, Lankapura
36	Divisional Secretariat, Matugama	203	Divisional Secretariat, Medirigiriya
37	Divisional Secretariat, Millaniya	204	Divisional Secretariat, Welikanda
38	Divisional Secretariat, Panadura	205	Divisional Secretariat, Dimbulagala
39	Divisional Secretariat, Walallavita	206	Divisional Secretariat, Thamankaduwa
40			KURUNEGALA - 30 DSs
	GALLE- 19 DSs	207	Divisional Secretariat, Kurunegala
41	Divisional Secretariat, Akmeemana	208	Divisional Secretariat, Giribawa
42	Divisional Secretariat, Ambalangoda	209	Divisional Secretariat, Galgamuwa
43	Divisional Secretariat, Baddegama	210	Divisional Secretariat, Ehetuwewa
44	Divisional Secretariat, Balapitiya	211	Divisional Secretariat, Ambanpola
45	Divisional Secretariat, Benthota	212	Divisional Secretariat, Kotavehera
46	Divisional Secretariat, Bope- Poddala	213	Divisional Secretariat, Rasnayakapura
47	Divisional Secretariat, Elpitiya	214	Divisional Secretariat, Nikaweratiya
48	Divisional Secretariat, Galle	215	Divisional Secretariat, Mahawa
49	Divisional Secretariat, Gonapinuwala	216	Divisional Secretariat, Polpithigama
50	Divisional Secretariat, Habaraduwa	217	Divisional Secretariat, Ibbagamuwa
51	Divisional Secretariat, Hikkaduwa	218	Divisional Secretariat, Ganewatta
52	Divisional Secretariat, Imaduwa	219	Divisional Secretariat, Wariyapola
53	Divisional Secretariat, Karandeniya	220	Divisional Secretariat, Kobeigane
54	Divisional Secretariat, Nagoda		

55	Divisional Secretariat, Neluwa	221	Divisional Secretariat, Bingiriya
56	Divisional Secretariat, Niyagama	222	Divisional Secretariat, Panduwasnuwara
57	Divisional Secretariat, Thawalama	223	Divisional Secretariat, Katupotha
58	Divisional Secretariat, Welivitiya - Divithura	224	Divisional Secretariat, Bamunakotuwa
59	Divisional Secretariat, Yakkalamulla	225	Divisional Secretariat, Maspotha
	MATARA - 16 DSs	226	Divisional Secretariat, Mallawapitiya
60	Divisional Secretariat, Kamburupitiya	227	Divisional Secretariat, Ridigama
61	Divisional Secretariat, Akuressa	228	Divisional Secretariat, Mawathagama
62	Divisional Secretariat, Athuraliya	229	Divisional Secretariat, Kuliypitiya East
63	Divisional Secretariat, Devinuwara	230	Divisional Secretariat, Weerambagedara
64	Divisional Secretariat, Dickwella	231	Divisional Secretariat, Kuliypitiya West
65	Divisional Secretariat, Hakmana	232	Divisional Secretariat, Udubaddawa
66	Divisional Secretariat, Kirinda_Puhulwella	233	Divisional Secretariat, Pannala
67	Divisional Secretariat, Kotapola	234	Divisional Secretariat, Narammala
68	Divisional Secretariat, Malimbada	235	Divisional Secretariat, Alawwa
69	Divisional Secretariat, Matara	236	Divisional Secretariat, Polgahawela
70	Divisional Secretariat, Mulatiyana		PUTTLAM - 16 DSs
71	Divisional Secretariat, Pasgoda	237	Divisional Secretariat, Puttalam
72	Divisional Secretariat, Pitabeddara	238	Divisional Secretariat, Kalpitiya
73	Divisional Secretariat, Thihagoda	239	Divisional Secretariat, Dankotuwa
74	Divisional Secretariat, Weligama	240	Divisional Secretariat, Karuwalagaswewa
75	Divisional Secretariat, Welipitiya	241	Divisional Secretariat, Chilaw
	HAMBANTOTA - 12 DSs	242	Divisional Secretariat, Pallama
76	Divisional Secretariat, Ambalantota	243	Divisional Secretariat, Mundel
77	Divisional Secretariat, Angunakolapelessa	244	Divisional Secretariat, Arachchikattuwa
78	Divisional Secretariat, Beliatta	245	Divisional Secretariat, Anamaduwa
79	Divisional Secretariat, Hambantota	246	Divisional Secretariat, Madampe
80	Divisional Secretariat, Katuwana	247	Divisional Secretariat, Nawagattegama
81	Divisional Secretariat, Lunugamwehera	248	Divisional Secretariat, Mahakumbukkadawala
82	Divisional Secretariat, Okewela	249	Divisional Secretariat, Mahawewa
83	Divisional Secretariat, Sooriyawewa	250	Divisional Secretariat, Nattandiya
84	Divisional Secretariat, Tangalle	251	Divisional Secretariat, Wennappuwa
85	Divisional Secretariat, Thissamaharama	252	Divisional Secretariat, Vanathavilluwa
86	Divisional Secretariat, Walasmulla		AMPARA - 20 DS's
87	Divisional Secretariat, Weeraketiya	253	Divisional Secretariat, Ampara
	MATALE - 11 DSs	254	Divisional Secretariat, Mahaoya
88	Divisional Secretariat, Ambangankorale	255	Divisional Secretariat, Dehiattakandiya
89	Divisional Secretariat, Dambulla	256	Divisional Secretariat, Padiyathalawa
90	Divisional Secretariat, Galewela	257	Divisional Secretariat, Uhana
91	Divisional Secretariat, Laggala -	258	Divisional Secretariat, Navithanveli

Pallegama		
92	Divisional Secretariat, Matale	259
93	Divisional Secretariat, Naula	260
94	Divisional Secretariat, Pallepola	261
95	Divisional Secretariat, Rattota	262
96	Divisional Secretariat, Ukuwela	263
97	Divisional Secretariat, Wilgamuwa	264
98	Divisional Secretariat, Yatawatta	265
	KANDY - 20 DSs	266
99	Divisional Secretariat, Akurana	267
100	Divisional Secretariat, Delthota	268
101	Divisional Secretariat, Doluwa	269
	Divisional Secretariat, Ganga Ihala	
102	Korale	270
103	Divisional Secretariat, Harispattuwa	271
	Divisional Secretariat,	
104	Hatharaliyadda	272
105	Divisional Secretariat, Kandy	
106	Divisional Secretariat, Kundasale	273
107	Divisional Secretariat, Medadumbara	274
108	Divisional Secretariat, Minipe	275
109	Divisional Secretariat, Panvila	276
	Divisional Secretariat, Pasbage	
110	Korale = Nawalapitiya	277
111	Divisional Secretariat, Pathadumbara	278
	Divisional Secretariat,	
112	Pathahewaheta	279
113	Divisional Secretariat, Poojapitiya	280
114	Divisional Secretariat, Thumpane	281
115	Divisional Secretariat, Udadumbara	282
116	Divisional Secretariat, Udapalatha	283
117	Divisional Secretariat, Uduuwara	284
118	Divisional Secretariat, Yatinuwara	285
	NUWARA ELIYA - 5 DSs	286
119	Divisional Secretariat, Ambagamuwa	287
	Divisional Secretariat,	
120	Hanguranketha	
121	Divisional Secretariat, Kothmale	288
122	Divisional Secretariat, Nuwara Eliya	289
123	Divisional Secretariat, Walapane	290
	KEGALLE- 11 DSs	291
124	Divisional Secretariat, Aranayake	
		Divisional Secretariat, Samanthurai
		Divisional Secretariat, Kalmunai
		Divisional Secretariat, Kalmunai (Tamil)
		Divisional Secretariat, Sainthamarathu
		Divisional Secretariat, Karativu
		Divisional Secretariat, Nintavur
		Divisional Secretariat, Addalachchenai
		Divisional Secretariat, Eragama
		Divisional Secretariat, Akkaraipattu
		Divisional Secretariat, Alayadiwembu
		Divisional Secretariat, Damana
		Divisional Secretariat, Thirukkovil
		Divisional Secretariat, Pottuvil
		Divisional Secretariat, Lahugala
		JAFFNA - 15 DSs
		Divisional Secretariat - Delft
		Divisional Secretariat - Island South,
		Velanai
		Divisional Secretariat - Kayts
		Divisional Secretariat - Karainagar
		Divisional Secretariat - Jaffna
		Divisional Secretariat - Nallur
		Divisional Secretariat - Valikamam South
		West, Sandilipay
		Divisional Secretariat - Valikamam West,
		Chankanai
		Divisional Secretariat - Valikamam South,
		Uduvil
		Divisional Secretariat - Valikamam North,
		Tellippalai
		Divisional Secretariat - Valikamam East,
		Kopay
		Divisional Secretariat - Thenmarachchi,
		Chavakachcheri
		Divisional Secretariat - Vadamaradchi
		South West, Karaveddy
		Divisional Secretariat - Vadamaradchi
		North, Point Pedro
		Divisional Secretariat - Vadamaradchi
		East, Maruthankerny
		KILINCHCHI - 4 DSs
		Divisional Secretariat - Pachchilaipalli
		Divisional Secretariat - Kandawali
		Divisional Secretariat - Karachchi
		Divisional Secretariat - Poonakary
		MULLAITIVU - 6 DSs

125	Divisional Secretariat, Bulathkohupitiya	292	Divisional Secretariat - Thunukkai
126	Divisional Secretariat, Dehiovita	293	Divisional Secretariat - Manthai East
127	Divisional Secretariat, Deraniyagala	294	Divisional Secretariat - Puthukudiyiruppu
128	Divisional Secretariat, Galigamuwa	295	Divisional Secretariat - Oddusuddan
129	Divisional Secretariat, Kegalle	296	Divisional Secretariat - Maritim Pattu
130	Divisional Secretariat, Mawanella	297	Divisional Secretariat - Welioya
131	Divisional Secretariat, Rambukkana		MANNAR - 5 DSs
132	Divisional Secretariat, Ruwanwella	298	Divisional Secretariat - Mannar Town
133	Divisional Secretariat, Warakapola	299	Divisional Secretariat - Manthai West, Adampan
134	Divisional Secretariat, Yatiyantota	300	Divisional Secretariat - Madu
	RATNAPURA- 17 DSs	301	Divisional Secretariat - Musali
135	Divisional Secretariat, Ayagama	302	Divisional Secretariat - Nanaddan
136	Divisional Secretariat, Balangoda		VAVUNIYA - 4 DSs
137	Divisional Secretariat, Eheliyagoda	303	Divisional Secretariat - Vavuniya
138	Divisional Secretariat, Elapatha	304	Divisional Secretariat - Vavuniya North
139	Divisional Secretariat, Embilipitiya	305	Divisional Secretariat - Vavuniya South
140	Divisional Secretariat, Godakawela	306	Divisional Secretariat - Vengalcheddiculam
141	Divisional Secretariat, Imbulpe		TRINCOMALEE - 11 DSs
142	Divisional Secretariat, Kahawatta	307	Divisional Secretariat - Gomarankadawala
143	Divisional Secretariat, Kalawana	308	Divisional Secretariat - Kantalai
144	Divisional Secretariat, Kiriella	309	Divisional Secretariat – Kinniya
145	Divisional Secretariat, Kolonna	310	Divisional Secretariat – Kuchchaveli
146	Divisional Secretariat, Kuruvita	311	Divisional Secretariat – Morawewa
147	Divisional Secretariat, Nivithigala	312	Divisional Secretariat – Mutur
148	Divisional Secretariat, Opanayaka	313	Divisional Secretariat - Padavi Sri Pura
149	Divisional Secretariat, Pelmadulla	314	Divisional Secretariat – Seruwila, Serunuwara
150	Divisional Secretariat, Ratnapura	315	Divisional Secretariat - Thampalakamam
151	Divisional Secretariat, Weligepola	316	Divisional Secretariat - Trincomalee Town & Gravets
	BADULLA- 15 DSs	317	Divisional Secretariat - Verugal, Echchalampattu
152	Divisional Secretariat, Badulla		BATTICALOA - 14 DSs
153	Divisional Secretariat, Bandarawela	318	Divisional Secretariat - Manmunai South and Eruvil Pattu, Kaluwanchikudy
154	Divisional Secretariat, Ella	319	Divisional Secretariat - Eravur Town
155	Divisional Secretariat, Haldumulla	320	Divisional Secretariat - Eravurpattu, Chenkalady
156	Divisional Secretariat, Hali-Ela	321	Divisional Secretariat - Kattankudy
157	Divisional Secretariat, Haputale	322	Divisional Secretariat - Koralai Pattu
158	Divisional Secretariat, Kandaketiya	323	Divisional Secretariat - Manmunai Pattu, Arayampathy
159	Divisional Secretariat, Lunugala	324	Divisional Secretariat - Koralaipattu North, Vakarai
160	Divisional Secretariat, Mahiyanganaya	325	Divisional Secretariat - Koralaipattu South, Kiran

161	Divisional Secretariat, Meegahakivula	326	Divisional Secretariat - Koralaipattu West, Oddamawadi
162	Divisional Secretariat, Passara	327	Divisional Secretariat - KoralaiPattu Central, Valaichenai
163	Divisional Secretariat, Rideemaliyadda	328	Divisional Secretariat - Manmunai South West.
164	Divisional Secretariat, Soranathota	329	Divisional Secretariat - Manmunai North, Batticaloa Town
165	Divisional Secretariat, Uva- Paranagama	330	Divisional Secretariat - Manmunai West - Vavunativu, Navatkadu
166	Divisional Secretariat, Welimada	331	Divisional Secretariat - Portheevu Pattu, Vellavelly

INSPECTION COPY

10 Implementation Schedule

No	Item:	Description:	Deadline:
1		Successful acceptance of the following 1 Completion of NDI hosting Infrastructure 2 Completion of the NDI software solution 3 Certificate Authority and related services 4 Delivery of Portable units 5 Related Reports	4 months from the contract effective date
2		Successful acceptance of the following 1 Establishment of enrolment stations at Colombo DS 2 Training of enrolment staff at Colombo DS 3 Delivery of (Phase 1) DTCs 4 Related Reports	4 months from the contract effective date
3		Successful UAT acceptance of the following; 1 User Acceptance Test (UAT) Certification	5 th month, from the contract effective date
4		Successful acceptance of the following 1 Establishment of enrolment stations at all other NDF center 2 Training of enrolment staff at all other NDF centers 3 Successful personalization of DTCs 4 Related reports 5 Monthly operational report	12 months from the date of successful UAT acceptance
5		Successful acceptance of the following 1 Household Transfer Management (HTM) system	8 months from the contract effective date
6		Successful Acceptance of the following; 1 Operation Acceptance Test (OAT) Certification	13 th month, from the date of successful UAT acceptance
7		Successful acceptance of the following 1 DTC (Phase 2) 1.1 Batches of 1 million DTCs (Phase 2) 1.2 Maximum of 14 batches.	Within 1 month from the date of employers request for a 1 million batch.
8		Successful Acceptance of the following; 1 Related reports 2 Monthly operational report	Delivered Quarterly during the 4-year operational time period.

11 General Requirements

Description	Bidders Compliance	Reference (Section No and Page NOs)
<p>11.1 General Technical Requirements</p> <p>11.1.1 Language Support: All information technologies must provide support for English, Sinhala and Tamil in Unicode fonts.</p> <p>11.1.2 DATES: All information technologies MUST properly display, calculate, and transmit date data, including, but not restricted to 21st-Century date data.</p> <p>11.1.3 Electrical Power: All active (powered) equipment must operate on: voltage range and frequency range, e.g., 220v +/- 20v, 50Hz +/- 2Hz . All active equipment must include power plugs standard in Sri Lanka.</p> <p>11.1.4 Environmental: Unless otherwise specified, all equipment must operate in environments of general Sri Lankan conditions.</p> <p>11.1.5 Bidder shall try to utilize existing local telecommunication infrastructure, as much as possible, in transferring traffic without affecting the required Service Levels.</p> <p>11.1.6 The Employer will NOT be responsible for the issuance of any licenses or authorizations required for this project for the Bidder. It is the responsibility of the Bidder to obtain required licenses in time to commence operations of the proposed solutions or form alliances with appropriate local licensed authorities to deliver the required services specified in project scope.</p> <p>11.1.7 The items listed as requirements and deliverables must be used only as guidance of the deliverables and not as a limiting factor to provide additional information required that may not be listed here.</p> <p>11.1.8 Bidder shall use their experience and best practices approach</p>		

<p>to provide any and all required information related to the assignment, beyond the items listed in this document if appropriate.</p> <p>11.1.9 Language Support: Shall confirm to localization standards of the Information and Communication Agency of Sri Lanka.</p> <p>11.1.10 DATES: All information technologies MUST properly display, calculate, and transmit date data, including, but not restricted to 21st-Century date data. System MUST be compliant with ISO 8601 Standard with regards to date / time.</p> <p>11.1.11 Electrical Power: All active (powered) equipment MUST operate on voltage range and frequency range of 220v +/- 20v, 50Hz +/- 2Hz . All active equipment must include power plugs standard in Sri Lanka.</p> <p>11.1.12 Environmental: Unless otherwise specified, all equipment MUST operate in environments of 10-30 degrees centigrade of temperature, 20 -80 percent of relative humidity and 0-40 grams per cubic meter of dust.</p> <p>11.1.13 Safety:</p> <p>11.1.13.1 Unless otherwise specified, all equipment installed at remote sites MUST operate at noise levels no greater than 55 decibels at 1m.</p> <p>11.1.13.2 All electronic equipment that emits electromagnetic energy MUST be certified as meeting US FCC class B or EN 55022 and EN 50082-1 or equivalent, emission standards.</p> <p>11.2 Adherence to common industry standards</p> <p>11.2.1 The software, hardware, network & communication technologies proposed by the bidder MUST be based on non-propriety and common industry standards whenever such standards are available and applicable.</p> <p>11.2.2 Any license required for the system shall be perpetual and shall cover installation and usage across all entities under the line ministry, provincial ministries ministry or at any</p>		
--	--	--

<p>other site where the proposed system or part of it is installed. All licenses shall not be based on number of users or sites.</p> <p>11.2.3 Standards used in the System shall be supported by more than one vendor and affirmed by a recognized standards body.</p> <p>11.2.4 The entire solution shall be web based and web-enabled and shall not require installation of any software / library at the employer systems.</p>		
--	--	--

INSPECTION COPY