Ministry of Public Security and Parliamentary Affairs of Sri Lanka

Department of Immigration and Emigration

PROCUREMENT DOCUMENT (Volume 2)

Section VI Schedule of Requirements

International Competitive Bidding (ICB)

Single Stage Two Envelope Bidding Procedure

Procurement of Issuance System and Relevant Public Key Infrastructure Components for Personalization of e-Passports to the Department of Immigration and Emigration of Sri Lanka

IFB No: DIE/PRO/PKI/2025

Employer:

Controller General,
Department of Immigration and Emigration,
5th Floor, "Suhurupaya", Sri Subhuthipura Road,
Battaramulla,
Sri Lanka.

April 2025

Contents

List of Acronyms

AA	Active Authentication
AES	Advanced Encryption Standard
BAC	Basic Access Control
CSCA	Country Signing Certificate Authority
CVCA	Country Verifiable Certificate Authority
CRL	Certificate Revocation List
CMAC	Cipher-based Message Authentication Code
DS	Document Signer
DVCA	Document Verifying Certification Authority
DES	Data Encryption Standard
DG	Data Group
DER	Distinguished Encoding Rule
EAC	Extended Access Control
ECDSA	Elliptic Curve Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
eMRTD	Electronic Machine-Readable Travel Document
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
IT	Information Technology
KMS	Key Management System
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MRZ	Machine Readable Zone
nPKD	National Public Key Directory
PA	Passive Authentication
PKI	Public Key Infrastructure

PKD	Public Key Directory
PCSC	Personal Computer / Smart Card
RBAC	Role-Based Access Control
RSA	Rivest-Shamir-Adleman
RSASSA-PSS -RSA	Signature Scheme with Appendix Probabilistic Signature Scheme
RSASSA-PKCS -RSA	Signature Scheme with Appendix Public Key Cryptography Standards
SAC	Supplementary Access Control
SHA	Secure Hash Algorithm
Sri Lanka CERT	Sri Lanka Computer Emergency Readiness Team
SOD	Document Security Object

Section VI Schedule of Requirements

1. Introduction

The Department of Immigration and Emigration in Sri Lanka was established in 1948. The Department of Immigration and Emigration Sri Lanka oversees the regulations of the country's border control and manages the movement of individuals in and out of Sri Lanka while issuing passports to Sri Lankan nationals. To execute the main functions of border control system of Sri Lanka the Department uses its own Border Control System with a reliable and standard passport issuing system, which serves as the identity of Sri Lankans while they are in overseas and facilitates them to cross international borders. The Department of Immigration and Emigration intends to commission the issuance of electronic passports (e-Passports) in compliance with ICAO standards, improve efficiency and effectiveness, and streamline the electronic passport issuance process.

2. Scope of Work

The key activities and services to be carried under the project described in this document include the following general scope

a. The Bidder shall design the Personalization and Issuance system with DI&E and install, test, commission all required components at the DI&E site as part of this contract.

b. The Bidder shall design a component to aggregate Demographic, Photo and Fingerprint data from different existing DI&E system and install, test, commission all required components for the system at the DI&E site as part of this contract.

c. The Bidder shall design the Public Key Infrastructure (PKI) with DI&E and install, test, commission all required components at the DI&E site as part of this contract.

d. The Bidder shall design the Quality Control system with DI&E and install, test, commission all required components at the DI&E site as part of this contract.

e. The Bidder shall design the Stock / Inventory Management system with DI&E and install, test, commission all required components at the DI&E site as part of this contract.

f. The Bidder shall design the National Public Key Directory (nPKD) system with DI&E and install, test, commission all required components at the DI&E site as part of this contract.

g. All the IT infrastructure, 3rd party software solutions including racks and peripherals relevant to above systems to provided as part of this contract.

h. All the relevant licensing charges including 3rd party software shall be included as part of this contract.

i. Bidder shall provide Training of DI&E personnel on operation of newly installed infrastructure/system above.

j. Bidder shall provide support and maintenance service for 5 years for components above including local onsite support.

k. Solution provided through this contract shall be able to successfully personalize ePassport selected by DI&E as per relevant ICAO 9303 (8th edition).

l. Infrastructure provided through this contract shall be able to integrate with existing DI&E monitoring system.

m. Title and the ownership of the components related to all infrastructure (including but not limited to the HSM components) shall be with the DI&E even after the completion of this contract.

n. Solution provided through this contract shall be flexible to expand to disaster recovery site in future.

o. Administrative privileges to be provided by the system for authorized users of DI&E and training to be given on the same.

p. Vendors has to define the core components (please refer implementation schedule under No.4)and the rest of the components given in the specifications separately. Core components are the components of the project which are mandatory and required to start the ePassport personalization as per ICAO 9303 (8th edition)

q. Minimum monthly commitment of E-Passports will be 60,000.

The bidders must provide comprehensive description of the solutions proposed to meet the technical requirements and scope of work above in their technical proposal. The technical proposal will be the basis of the technical evaluation to evaluate whether bidders meet the technical requirements.

3. Governing Regulations

Solution provided under this contract shall be in compliance with ICAO 9303 (8th edition).

5. Implementation Schedule

The complete system shall be implemented as below.

L. No	Description/ Phase	Delivery Date / From the Date of Commencement (T)
1	Requirement finalization, workshop and final requirement approval	T+ 1 month
2	**Phase 1:** Design, install, test, commission all required core components required to start personalization of ePassport as per ICAO 9303 (8th edition). Include Core components Core components are : 1. KMS, HSM 2. Document Signer 3. CSCA 4. CVCA 5. DVCA 6. Personalization Solution Manager with data aggregation, data preparation as per Sri Lanka e-Passport requirement. 7. Personalization Station Software to drive / interface / control the existing printing machine from DIE to personalize the e-Passports. 8. Integration with three input database system(Demographic, Photo and Fingerprint) 9. QC with mandatory feature to test Sri Lanka e-Passport personalization. 10. All the relevant IT hardware, software, database, 3rd party license for above components. 11. Sri Lanka CERT security assessment	T+6 months
L. No	**Phase**	**Delivery Date**
3	**Phase 2:** Design, install, test, commission all remaining components required in this contract Remaining components are : 1. Personalization solution: Remaining all requirement described in compliance table other than already delivered as core components. 2. QC : Remaining all requirement described in compliance table other than already delivered as core components. 3. Inventory management system 4. nPKD 5. Scaling/ expansion of core components to full size for High availability	T+ 11 months.

	6. All the related IT hardware and software, 3rd party license etc. 7. Sri Lanka CERT security assessment	
4	**Operational Period** Issuance System and Relevant Public Key Infrastructure components for personalization of e-Passports and Issuance of personalized e-passports. Contractor shall perform services as per the SLA stipulated in Section VI: Schedule of Requirement until completion of Issuance 3,150,000 nos.	T+11 to T+60

5. Existing Printing Machine details

Printers	Model	Manufacture Year	Quantity
Diletta	900i	2021	17

6. Acceptance and Testing

Bidder need to provide criteria for Acceptance and Testing procedure to be followed between DI&E and bidder in their proposal. This shall include User Acceptance Test (UAT) and Operational Acceptance (OAT) of system before go live.

7. Functional & Non-functional Technical Requirements& Compliance

The Technical specification may be provided in the following format. The bidder shall fill the columns 3 and 4, and **must submit with the Technical Proposal**. The bidder’s failure to provide the information request in columns 3, 4 and 5 may be a reason for the rejection of the Bid. If any discrepancy is observed between the information provided by the bidder in columns 3, 4 and 5 and the other technical information attached to the bid, the information provided herein shall take precedence.

	(1)	*(2)*	*(3)*	*(4)*	*(5)* *Reference to the Technical BID*
	Technical Specifications and Standards				
	Purchaser's Requirements		*Bidder's Offer*		
	Detail	*Priority*	*Yes (Y)/ No (N)*	*Remarks*	
1. Functional Requirements for PKI System					
1.1	The PKI solution shall include CSCA, DS, CVCA, DVCA, nPKD (including interface to ICAO PKD), KMS, HSM.	Critical			
1.2	The CSCA, DS, CVCA, DVCA, nPKD (including interface to ICAO PKD), KMS, HSM shall be provided by the winning Bidder.	Critical			
1.3	The technical specifications related to PKI infrastructure and activities relating to management of Country Signing Certificates and Document Signing Certificates must be carried according to specification and guidelines issued by ICAO 9303 for the PKI functions, infrastructure and realization of key management.	Critical			
1.4	Format and structure of the PKI certificate (e.g. CSCA) of the DI&E to be shared with ICAO and other countries shall comply with the ICAO PKD requirements	Critical			
1.5	The selected Bidder must facilitate and guide the DI&E in relation to the formalities required in obtaining the ICAO-PKD membership (including preparation of the relevant documents, reports, samples).	Critical			
1.6	The proposed solution shall provide the total management of keys and certificates used to sign personalized eMRTD. The solution shall handle all aspects of key, certificate creation, management, revocation and associated policies in a very flexible and user-friendly manner	Critical			

	(1)	*(2)*	*(3)*	*(4)*	*(5)*
1.7	The proposed solution shall be compliant to ICAO Doc 9303 and specify the eMRTD PKI profile including: roles and responsibilities of entities in the infrastructure, cryptographic algorithms and key management, certificate and CRL content, certificate and CRL distribution mechanisms and, certification path validation.	Critical			
1.8	The proposed solution shall provide key life-cycle management like generation, import, export, certification, storage, back-up, restore, usage, expiry, update, renew, version control and revocation features. These functions must be provided in compliance with ICAO standard and guidelines for eMRTD	Critical			
1.9	All CSCA certificates shall be self-signed certificates issued directly by the CSCA. Both the CSCA certificates and Document Signer certificates are associated with a private key usage and a public key validity period as outlined in ICAO 9303	Critical			
1.10	The proposed solution shall have capability for CSCA key pair be replaced every three years.	Critical			
1.11	For use in the CSCA and DS the Key Management modules shall support below algorithms: a. Rivest, Shamir and Adleman (RSA) b. Elliptic Curve Cryptography (ECC)	Critical			
1.12	The proposed solution shall support the same algorithm for use in CSCA and DS. It shall be possible to choose appropriate key lengths offering protection against attacks considering suitable cryptographic catalogues	Critical			
1.13	The PKI system shall support DI&E to distribute the below ICAO PKI objects. a. CSCA certificates b. Document Signer certificates c. CRLs (null and non-null)	Critical			

	(1)	*(2)*	*(3)*	*(4)*	*(5)*
14	The PKI system shall provide a plan of the key pair rollover strategies for both CSCA keys and DS keys to enable propagation of certificates and CRLs. The solution must support uploading certificates; CRLs to the ICAO provided PKD service using the Lightweight Directory Access Protocol (LDAP) to the Write Directory. Further the proposed solution shall automate the storage and exchange of national certificates and revocation lists with PKD of ICAO	Critical			
1.15	The solution shall issue certificates and CRLs that conform to the profiles specified in ICAO 9303. All certificates and CRLs shall be produced in Distinguished Encoding Rule (DER) format as specified by ICAO 9303 to preserve the integrity of the signatures within them.	Critical			
1.16	The proposed solution shall be capable of generation and maintenance of keys and certificates for CVCA supporting the issuance of eMRTD with Extended Access Control (EAC).	Critical			
1.17	The proposed solution must provide certificates for Extended Access Control usages in ePassport based on LDS1 or LDS2. The proposal shall include at least the following modules that should comply with the latest release of BSI TR-03110 and ICAO Doc 9303 8th edition. ○ Country Verifying Certificate Authority (CVCA) ○ Document Verifying Certificate Authority (DVCA) ○ Administrative Certificate Authority for officer authentication, machine to machine authentication	Critical			

	(1)	*(2)*	*(3)*	*(4)*	*(5)*
1.18	The CVCA, CVCA link, DVCA and IS certificates MUST be in a card verifiable format. ○ The certificate format and profile should be as specified in Appendix C.1 of TR-03110 and ICAO Doc 9303 8th edition. ○ The solution shall support CVCA key rollover. ○ The solution should be able to sign DV and IS certificate requests following a profile as specified in Appendix C.2 of TR-03110. ○ The solution should support authorizations for certificate holders as CVCA, DV, IS with read access rights to DG3 (Fingerprint).	Critical			
1.19	The DS of the personalization solution shall be used to sign Document Security Object (SOD) to create a digital signature protecting the authenticity and integrity of the eMRTDs according to ICAO 9303.	Critical			
1.20	The DS shall have an interface to the KMS to securely perform required cryptographic operations	Critical			
1.21	The DS shall be agnostic to CSCA.	Critical			
1.22	The DS shall allow to sign multiple types of eMRTD (Ordinary, Official, Diplomatic) with RSA and ECDSA key generation parameters and algorithms	Critical			
1.23	The DS shall be able to define key validity by time period or maximum number of signature generation or the combination of both.	Critical			
1.24	The DS shall verify the validity/consistency of the input Data Group (DG) provided such as DG1 data, country code, issuance date before proceeding to signature generation.	Critical			

	(1)	*(2)*	*(3)*	*(4)*	*(5)*
1.25	The DS shall provide an interface for monitoring purpose of the active keys and number or remaining signatures.	Critical			
1.26	The DS shall have Role-Based Access Control (RBAC) to manage the various user roles and their access to system functionalities.	Critical			
1.27	The DS shall maintain comprehensive audit trails. Logging activities, user actions and changes made within the system shall be tracked to ensure accountability and facilitate investigations.	Critical			
1.28	The KMS shall be used to ensure the security of sensitive data and securely generate any cryptographic data.	Critical			
1.29	The KMS of the personalization solution shall operate in a secure environment to handle key management functions required for electronic passport documents including, but not limited to, keys generation, certification requests, signing, encryption, and decryption operations by using a dedicated Hardware Security Module (HSM).	Critical			
1.30	The HSM shall provide functionality modules to allow secure integration between the KMS and the HSM by executing the KMS firmware within the secure confines of the HSM.	Critical			
1.31	The HSM shall be at least FIPS 140-2 Level 3 validated or Common Criteria EAL4+ certified.	Critical			
1.32	The KMS shall provide online access and API for cryptographic operations/functions that are needed during the personalization step and quality control, to authenticate with the chip and perform necessary cryptographic operations.	Critical			

	(1)	(2)	(3)	(4)	(5)
1.33	The KMS shall support the following algorithms: 1) Symmetric Cryptographic algorithms a. 3DES b. AES up to 256 2) Asymmetric Cryptographic algorithms a. RSA keys up to 4096 bits b. ECC keys up to 521 bits 3) Signature mechanisms a. RSASSA-PSS b. RSASSA-PKCS-v1_5 c. ECDSA 4) Hashing mechanisms a. SHA-224 b. SHA-256 c. SHA-384 d. SHA-512 e. DES-MAC f. 3DES-MAC g. AES-CMAC	Critical			

1.34	The KMS shall allow secure key import, export, backup and restore functionalities. The keys shall not be exposed in unencrypted form outside the HSM during the above functionalities.	Critical			
1.35	The KMS shall be able to manage Keys lifecycle and obsolescence.	Critical			
	(1)	*(2)*	*(3)*	*(4)*	*(5)*
1.36	The KMS shall have a secure database to store the cryptographic keys	Critical			
1.37	The KMS shall provide a Graphical User Interface (GUI) to manage the cryptographic keys.	Critical			
1.38	The KMS shall have Role-Based Access Control (RBAC) to manage the various user Roles and their access to system functionalities. It shall support Dual Control for access to the most secure data or functionalities	Critical			
1.39	The KMS shall maintain comprehensive audit trails. Logging activities, user actions and changes made within the system shall be tracked to ensure accountability and facilitate investigations.	Critical			

	2. Functional Requirements of Personalization Solution				
2.1	The personalization solution shall be modular and scalable to accommodate higher volumes and enable easy update in the future	Critical			
2.2	The personalization solution shall be composed of separate modules of which each of the module handles their own separate tasks	Critical			
2.3	The personalization solution shall be made-up of server applications and client applications	Critical			
2.4	The personalization solution shall be able to interface with other systems (e.g. KMS, PKI) over secure and standard web-based interfaces	Critical			
	(1)	*(2)*	*(3)*	*(4)*	*(5)*
2.5	The personalization solution shall use dedicated and customizable connectors for communication with external systems (e.g. KMS, PKI) to facilitate easy integration with external systems	Critical			
2.6	The personalization solution shall integrate with a Key Management System	Critical			
2.7	The personalization solution shall integrate with a Document Signer system.	Critical			
2.8	The personalization solution shall integrate with a Quality Control system.	Critical			

2.9	The personalization solution shall include and integrate with an Inventory Management system.	Critical			
2.10	The personalization solution shall interface with a relational database to handle the data persistence required to run correctly and effectively the personalization process	Critical			
2.11	The personalization solution shall support centralized, distributed and mixed issuance scheme	Critical			
2.12	Any server applications shall be developed using Java technology or other similar open source	Critical			
2.13	Server applications shall support Windows Server or Linux Server	Critical			
	(1)	*(2)*	*(3)*	*(4)*	*(5)*
2.14	All web interfaces shall be supported on at least 3 (three) of the most popular web browsers available in the market.	Critical			
2.15	Client applications shall support Windows operating system.	Critical			
2.16	Any client applications shall be developed using .NET framework or other similar technologies on windows platform.	Critical			
2.17	The personalization solution shall be provided with the database system required.	Critical			

2.18	A web interface shall be provided to configure the personalization solution.	Critical			
2.19	The personalization solution shall enable traceability of all user and system actions in audit logs in order to track “who did what, at what time”. The personalization solution may separate the audit logs from the application logs.	Critical			
2.20	The personalization solution shall provide an in-built ‘application request priority management’ functionality enabling the customer to arrange application requests in a prioritized manner.	Critical			
	(1)	*(2)*	*(3)*	*(4)*	*(5)*
2.21	The personalization solution shall provide functionality to sort/order application requests according to any order criteria including, but not limited to, priority order, and to create batches containing the application requests according to the order criteria and pre-set maximum batch size.	Critical			
2.22	The personalization solution shall provide functionality to create manual batching of application requests	Critical			
2.23	The personalization solution shall be personalization machine suppliers independent.	Critical			
2.24	The personalization solution shall be possible to integrate with different personalization machine suppliers in the market provided machine is compliant with relevant ISO 14443, ISO 7816 communication protocols.	Critical			

2.25	The personalization solution shall be PKI suppliers independent so that future change in PKI system shall be possible to integrate with personalization solution.	Critical			
2.26	The personalization solution shall provide customizable production dashboard containing the most important production KPIs in one central point of access in order to track and optimize the production quality. The content of the dashboard shall be configurable per user role.	Critical			
2.27	The personalization solution shall provide a set of production listing & reports allowing the operator to track easily the production processes from stock retrieval to delivery	Critical			
	(1)	*(2)*	*(3)*	*(4)*	*(5)*
2.28	The personalization solution shall enable exporting of the report into different file format including, but not limited to, PDF and EXCEL files format.	Critical			
2.29	The personalization solution shall enable printing of the report.	Critical			
2.30	The personalization solution shall provide production statistics according to the requirement including, but not limited to, yearly, monthly and weekly production statistics	Critical			
2.31	The personalization solution shall rely on Active Directory for the user or role management	Critical			
2.32	The personalization solution shall support user authentication through LDAP or LDAPS.	Critical			

2.33	The user interfaces of the personalization solution shall be role-based, providing different user interfaces and functions depending on the user role.	Critical			
2.34	The personalization solution shall provide search functions to get access to the relevant history information including, but not limited to, the history of application requests, batches and documents	Critical			
2.35	The personalization solution shall implement a mechanism to prevent the personalization of duplicate application requests	Critical			
2.36	The personalization solution shall notify the system issuing the application personalization requests about the corresponding document personalization or production result.	Critical			

	(1)	*(2)*	*(3)*	*(4)*	*(5)*
2.37	The personalization solution shall be dynamically configurable to securely delete any personal data within a pre-defined data retention period after document production. The employer will define the timeline for data retention. The retained data should be accessible in a readable format with proper approval and logs should be available for review.	Critical			
2.38	The personalization solution shall provide an option to protect confidentiality of the database	Critical			
2.39	The personalization solution shall protect confidentiality of the production data file.	Critical			
2.40	The personalization solution shall be compliant to International General Data Protection Regulation (GDPR).	Critical			
2.41	The personalization solution shall be developed following a framework of Secure Development Life Cycle process.	Critical			
2.42	The personalization solution shall provide a component to aggregate Demographic, Photo and Fingerprint data from different existing DI&E system.	Critical			
3. Functional Requirements of Quality Control (QC) System					
3.1	Quality Control system shall ensure quality of overall personalization process.	Critical			
3.2	Quality Control system shall be a standalone application used to check personalized e-Passports. It shall support the quantity of e-Passports to be verified per batch by configuration.	Critical			

	(1)	*(2)*	*(3)*	*(4)*	*(5)*
3.3	Quality control system shall carry out vital controls and verifications of both visual and electrical aspects of e-Passports.	Critical			
3.4	During the control, all of the following functionalities shall be verified: a) Manual visual control of the passport (logo, printing, security features). b) Passport compliancy with the ICAO standards. c) Verification of electrical data versus graphical data – ensure that data stored in the chip match with data printed on the e-Passport data page. d) Verification of electrical data versus production data – ensure that data stored in the chip match with the production data associated with the e-Passport.	Critical			
3.5	The system shall support full verification of ICAO document (BAC, SAC, AA, PA, EAC).	Critical			
3.6	The system shall verify MRZ and read data groups, including reading biometrics related Data Group (DG3) through EAC protocol.	Critical			
3.7	The system shall compare MRZ and DG1 in chip.	Critical			
3.8	The system shall display all the electrical data.	Critical			
3.9	The system shall be deployed in connected mode with production system and shall notify production system on e-Passport control result.	Critical			
3.10	The system shall control by batch with a minimum of verification according to configured threshold.	Critical			

	(1)	*(2)*	*(3)*	*(4)*	*(5)*
3.11	The system shall support view of available batches for control.	Critical			
3.12	The system shall support contactless PCSC reader, full page scanners, MRZ readers.	Critical			
4. Functional Requirement for Inventory Management system					
4.1	Inventory Management system shall manage stock article life-cycle from article reception to removal and reconciliation.	Critical			
4.2	Inventory Management system shall provide a convenient method on how information of incoming batches of blank e-Passport booklets can be captured into the system in a hassle-free manner for Inventory purposes.	Critical			
4.3	Inventory Management system shall manage • Stock movement from DI&E storage to the production area. • Stock relocation.	Critical			

4.4	Inventory Management system shall manage • Adjusts stock quantities according to need. • View articles as a list or split by different filters according to the search needs. • Displays articles on various categories such as stock-on-hand, re-order point. • Manages and tracks lost article. • Declares an article as damaged with the corresponding reason for tracking. • Keeps track of booklets rejected due to faults/defects both pre and post personalization.	Critical			
	(1)	*(2)*	*(3)*	*(4)*	*(5)*
4.5	Inventory Management system shall manage physical inventories by executing process for counting at a specific location or sub-location.	Critical			
4.6	Inventory Management system shall manage physical destruction process of secure documents with generation of certificate of destruction.	Critical			
4.7	Inventory Management system shall manage security: • Track all stock transactions so that you can see who has done what and when • Supports dual-control mechanism for sensitive operations such as stock removal, transfer and reconciliation.	Critical			
4.8	Inventory Management system shall be • Able to be deployed as a stand-alone application without any dependency with other modules • Built on OPEN API standard model • Able to be integrated with other ERP system.	Critical			

4.9	Inventory Management system shall •Supports different formats of barcode. •Supports multiple unit of measures defining the way stock articles are packaged, quantified and tracked (palette, box, bundle) • Supports supplier management.	Critical			
4.10	Inventory Management system shall • Issue alerts when stock level is below the safety stock • Issue alerts when a stock item becomes unfit for use (shelf-life) • Issue alerts when it is time to place a new order (reorder point) • Supports UI based alert channel.	Critical			
	(1)	*(2)*	*(3)*	*(4)*	*(5)*
4.11	Inventory Management system shall notify external system on specific stock events (stock entry, stock removal).	Critical			
4.12	Inventory Management system shall have feature (via Reports or otherwise) to allow officers to regularly tally or take stock of the booklets in their respective custody.	Critical			

5. General Requirements of Overall Solution

5.1	The selected bidder must supply and maintain all specialized and general hardware/software components that are required to fully implement the PKI infrastructure as per ICAO 9303 recommendations. Below minimum hardware and software shall be provided by the selected bidder. a. Physical Servers & Storage b. Virtualization c. Operating Systems d. Databases e. Switches f. Hardware Security Modules (HSM) g. Server Racks and accessories h. Quality Control peripherals (e-Passport readers, barcode scanners)	Critical			
5.2	System shall include all the other components required like firewall, anti-virus, load balancer, Backup solution, End Point Protection required to execute personalization of e-Passport securely.	Critical			
5.3	The infrastructure must be fully hosted within the territory and jurisdiction of Sri Lanka at a location agreeable to the DI&E. The DI&E shall have full ownership of the title, authority and access to such equipment, without any reservation or restriction from the date of commissioning of the new system.	Critical			
	(1)	*(2)*	*(3)*	*(4)*	*(5)*
5.4	Proposed Solution architecture (Production site) provides High Availability of 99.50% uptime. a. Software level b. Database level c. Server hardware level.	Critical			

5.5	Proposed solution shall handle minimum of 5,000 booklets data preparation requests within 7 hours (Active shift) for Production site. The solution shall be able to handle peak volume of 1,000 requests per hour.	Critical			
5.6	The selected bidder shall install and integrate proposed system with existing DI&E systems.	Critical			
5.7	The selected bidder shall propose the trainings for the administration, operation and supporting teams.	Critical			
5.8	The selected bidder shall provide five years warranty (including support and maintenance) for third-party software and hardware. All proposed hardware must be brand new and software must be latest version.	Critical			
5.9	The selected bidder shall provide 5 years of operation, support and maintenance for proposed issuance and PKI system.	Critical			
5.10	Security assessment from Sri Lanka CERT prior to go live	Critical			

8. Minimum Qualifications of Key Professional Staff

The Bidder shall provide the team of key professionals with the curriculum vitae and the team organization.

Core Project Team Key Professionals

No	Key Professional Staff	Academic and Professional	No of People	Total Experience in the Proposed Role /Years	Specific Experience with the Similar Area / Years	Specific Qualifications/Requirements
1	Project Manager	BSc in Computer Science, IT, or equivalent, and MBA or MSc or equivalent.	1	10	5	Proven track record in managing large-scale government IT projects, particularly in e-passport or PKI systems. Certification in project management such as PMP, PRINCE2, PMI-ACP®, or similar (Scrum certification preferred)is a plus.
2	Solution Architect	BSc in Computer Science, IT or equivalent, and MSc or equivalent.	1	10	5	Experience in designing and implementing PKI solutions for applications, including secure authentication, encryption, and digital signatures for e-passports.
3	PKI Specialist	BSc in Computer Science, IT or equivalent, or a related field.	1	6	5	In-depth experience in designing, implementing, and managing PKI solutions, including secure certificate management, cryptographic algorithms, and compliance with ICAO and other international standards.
4	Business Analyst	BSc in Computer Science, IT or equivalent and MSc or MBA	1	8	5	Demonstrate business analysis experience in e-Passport, PKI solution and eGovernment Information System related Projects.

		or equivalent. IIBA® Certification preferred.				
5	Security Architect	BSc in Computer Science, IT, Cybersecurity, Information Security, or equivalent.	1	8	5	Extensive experience in designing and implementing security frameworks for government digital systems including the application of cryptographic standards, secure data transmission, and regulatory compliance for e-passports.
6	System Administrator	BSc in Computer Science, IT, or equivalent.	1	8	5	Proven experience in the administration of secure IT infrastructure, managing both hardware and software systems required for secure PKI and e-passport applications.
7	Network Engineer	BSc in Network Engineering, Computer Science, or equivalent.	1	8	5	Cisco Certified Network Associate (CCNA), Certified Information Systems Security Professional (CISSP), or equivalent. Experience in designing and managing secure networks, with expertise in VPNs, firewalls, network security, and integration with e-passport systems.
8	Software Developer	BSc in Computer Science, Software Engineering, or equivalent.	2	8	5	Strong background in developing secure applications for e-passports, with expertise in relevant technologies. Proficiency in cryptographic modules and secure coding practices is a must.
9	Quality Assurance Lead	BSc in Computer Science, IT or equivalent.	1	8	5	Experience in quality assurance for high-security applications, including testing for compliance, performance, and security

						vulnerabilities. Expertise in automated testing frameworks and penetration testing is required.
10	Quality Assurance Engineer	BSc in Computer Science, IT or equivalent.	1	6	4	Experience in quality assurance for high-security applications, including testing for compliance, performance, and security vulnerabilities. Expertise in automated testing frameworks and penetration testing is required.
11	Training Expert	BSc in IT or related field. Certification Learning & Development, or equivalent	1	6	4	Experience in designing and delivering training for large-scale IT, security, or government digital transformation projects. Expertise in training delivery, change management, and on boarding programs

09. Facilities Provided by the Department of Immigration & Emigration

a. Data centre & Office space to host relevant IT equipment.

b. Ensure Power, electricity, Air Conditioning, access control availability to the office space to maintain SLA.

c. Ensure Network availability (connection to the DC racks) to maintain SLA

d. Access to Data centre for vendor support engineers

e. Physical and logical security, air conditioning, air, fire detection and suppression for the DC

f. Office space , chair table availability for L1 support engineers

g. Ensuring the support and software update from existing database vendors to integrate with the new personalization system.

h. Cooperation during workshop and integration with vendors

i. Arranging sample ePassport booklet for development testing and UAT testing.

j. Providing access to existing ePassport printers for the development and integration stage.

k. Providing SDK for existing ePassport printers

l. Ensuring availability of test data during development stage

m. All the required data for personalization in ePassport to be provided as per ICAO 9303 recommended format

n. Data for personalization needed with unique ID or Token no of each data record which can be used to identify requests

o. Deciding who will take the role of Security officers from DI&E for Key ceremony

p. DI&E officer availability for timely Signing of DS certificate by CSCA.

10. Training Approach

Training Module	**Details**	**Target Group**	**No. of Staff**	**Duration (Days)**	**Delivery Method Workshop/Hands-on/Online/Practical etc)**	**Materials**
Introduction to PKI & e-Passport	Overview of PKI, digital certificates, encryption, and signing in the e-Passport system	IT Security, Passport Issuance Team				
Certificate Authority (CA) Operations	Setup, management, and maintenance of the CA for e-Passport	IT Security, PKI Admins				
Key Management & HSM Operations	Secure key generation, storage, and lifecycle management using HSM	IT Security, PKI Admins				
e-Passport Issuance System	Process of issuing digitally signed e-Passports, key signing procedures	Passport Issuance Team, IT Support				

PKI Infrastructure Security & Compliance	Security policies, risk management, and compliance requirements	IT Security, Compliance Officers				
Incident Response & Disaster Recovery	PKI failure scenarios, certificate revocation, and recovery plans	IT Security, NOC Team				
Interoperability & Integration	PKI integration with border control, visa systems, and international standards	IT Security, System Integration Team				

11. Exit Criteria for PKI Solution of e-Passport Implementation

1. **Data Transfer Completion**

- All PKI-related data, including certificate authorities (CAs), keys, logs, and transaction records, should be transferred to the designated entity or nominated party by the department at least three months before the project's end or any other specified date during the project period. All license applicable will be renewed by employer on contract completion.
- The data to be transferred in secure manner for Keys and Certificates.

2. **Hardware and Software Component Handover & Procurement Record**

- All hardware &Software application components, including **HSMs (Hardware Security Modules), servers, security appliances, and workstations**, must be transferred to the department as part of the project scope. All license applicable will be renewed by employer on contract completion.
- The department should have full ownership of the hardware and software application, and procurement records should be shared, including **asset registration, serial numbers, and licensing details**.

3. **Documentation Submission**

The following updated and finalized documents must be submitted before project closure:

- **PKI System Architecture Diagram** (latest version with all changes incorporated)

- **Implementation Diagram** (detailing the setup, connections, and security layers)
- **PKI Policies and Procedures** (Certificate Policy (CP) and Certification Practice Statement (CPS))
- **Installation, Configuration, and Administration Manuals**
- **Security and Compliance Reports**
- **Any applicable disaster recovery and business continuity plans**

4. **System Validation & Acceptance**

- A final verification should be conducted to ensure that the transferred data, hardware, and documents are complete and functional, 3 months before end of contract period.
- The department should sign off on the project closure after confirming that all exit criteria have been met and that the PKI solution is **operational and maintainable**.

12. Performance requirements for the system

Following table 1 defines the key performance indicators for monitoring and measuring the performance of the systems and related impact on payments to be made by the purchaser. Following provides definitions of terms used in the system performance indicators.

The SLA parameters shall be measured on the availability of system in business days and the SLA reports shall be made available to the purchaser at the same time.

The penalties shall be calculated based on the percentage of the volume of passports/transactions affected.

Table 1: Annual Performance Indicators

S.N	SLA Parameter	Annual Performance Achieved (%)	% of Penalty
1.1	Availability of Personalization Solution and In-built Reporting module	<99.50	For each 0.1% drop in performance from the required level, 0.001% Contract Price penalty will be imposed.
1.2	Availability of Inventory Management system	<95.00	
1.3	Availability of Key Management System (KMS) and Hardware Security Module (HSM)	<99.50	
1.4	Availability of Country Signing Certification Authority (CSCA)and Country Verifying Certification Authority (CVCA)	<95.00	
1.5	NPKD (interfacing with ICAO PKD)	<99.50	
1.6	Availability of Document Signer (DS)/Document Verifying Certification Authority (DVCA)	<99.50	
1.7	Availability of Quality Control (QC) software	<99.50	
1.8	Availability of Personalization Software for Workstation	<99.50	
1.9	Data Centre Hardware Systems	<99.50	
1.10	Data Centre Platform Software	<99.50	
1.11	Information Security Applications	<99.50	

Table 2: Daily Performance Indicators

S.N	SLA Parameter	Performance Achieved	% of Penalty
1.1	Daily availability of Personalization Solution and In-built Reporting module RTO should be less than 20 minutes.	20 minutes/day	Recovery time objective (RTO) is set at 20minutes with zero data loss. 1% penalty will be imposed on the monthly bill for every 5-minute delay beyond the RTO.

Table 3: Support Levels

Support Level	SLA Parameter
2.1 First and Second Level Service Support (L1 and L2 Support)	• Acknowledge incidents • Logs, categorizes, prioritizes, tracks, and routes incidents reported by end users • Tracks and keep purchaser updated on the raised tickets until successfully resolved • Implement issue-fixes along the lines of a documented set of instructions • Diagnose for root cause analysis • Technical consultancy to implement workaround to relieve the pain of the issue • Configuration changes to fix any issues which are not due to new functionality requirements • Test and deployment of fix releases • Preventive maintenance including health check should be done in every agreed time period This includes the firmware updates as recommended by each product vendor in par with compatibility to versions implemented. In addition, it includes the software bug fixes as provided by software/hardware vendors.
2.2 Third Level Service Support (L3 Support)	The principals shall deliver operational and maintenance support for the software/hardware, which will cover bug fixes of the application software, defected hardware replacement, production support and access to regular product updates etc.

Table 4: Severity Levels

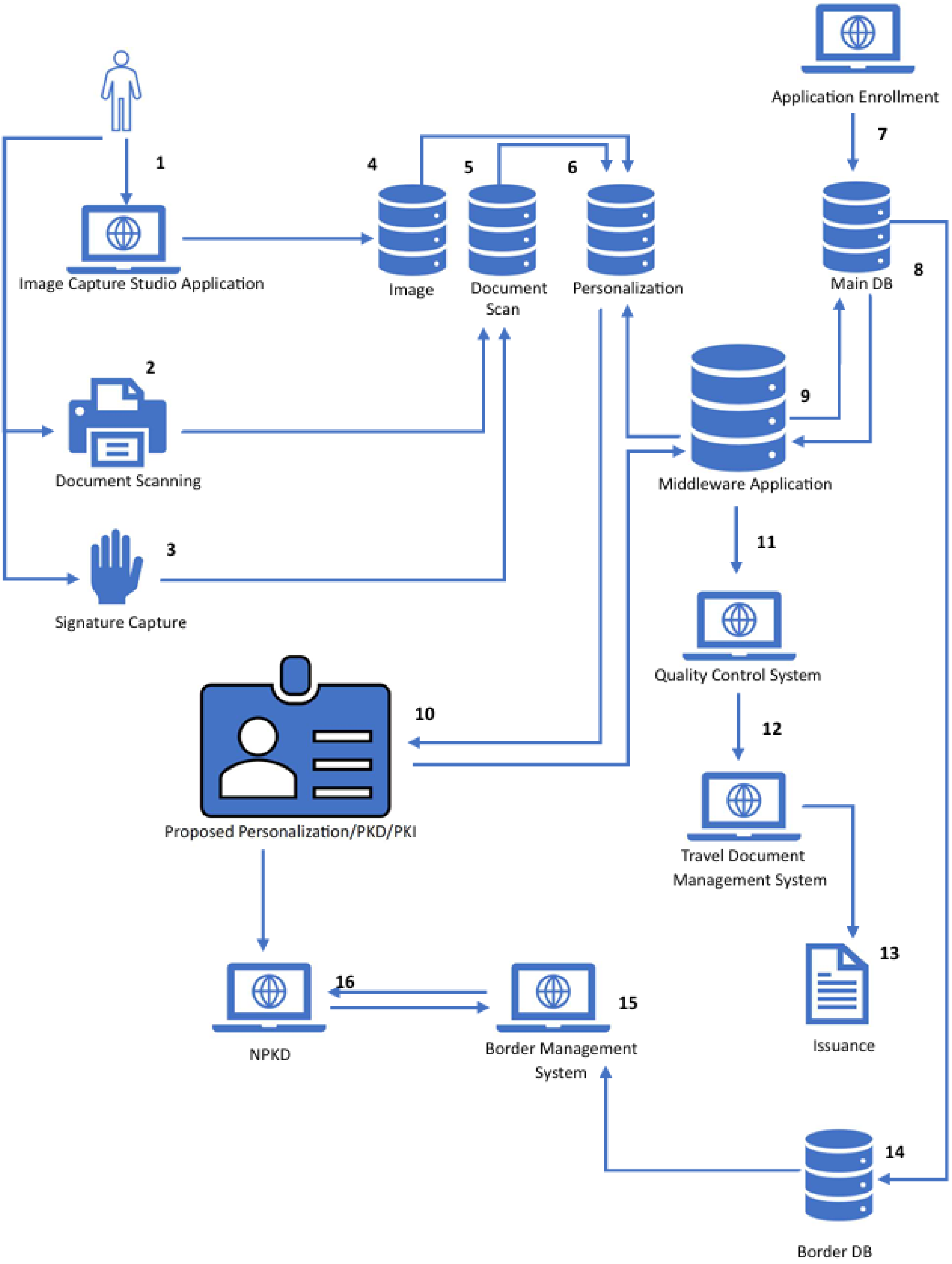
Severity	SLA Parameter	Initial Response	Performance Achieved (%)
3.1 Critical	Complete malfunction of the Software and loss of critical functionality of the system. The business impact is severe and no workarounds available. Ex: Total system inoperable	15Minutes	Attend immediately and will put commercially reasonable effort to restore the service to its workable condition on highest priority. 24x7 continuous effort until service is restored on best effort basis.
3.2 High	Loss of the use of the Software and loss of critical functionality of the system. The business impact severe and there is a workaround available. Ex: majority of the major system functionally are unusable.	30 Minutes	Resolution within 2 hours and will put commercially reasonable effort to restore the service to its workable condition on best effort basis
3.3 Moderate	Minimal interruption of the Software functionality and has a minor impact to business.	2 business days	Resolution within 3 business days and will put commercially reasonable effort to restore the service to its workable condition
3.4 Low	It may be a minor problem, a documentation error or minor incorrect behaviour that does not prevent operation of the Software or Hardware and access to the system major functionalities	7 business days	Resolution shall be in next maintenance release or via change request procedure as mutually agreed with customer

Annexure :1

e- Passport High Level Technical Specifications

1. Number of Pages : ePassport will be of 48 pages and with eCover (chip and antenna in cover)
2. The page structure :The composition, size, layout, and other related parameters of the e-passport will comply with the ICAO DOC 9303 specifications.
3. The ePassport will come with sewed in thin heat security laminate of less than 15micron thickness and carrier. The security laminate attachment to Datapage is after the graphical personalization.
4. Dimensions of ePassport ID-3 125mm x 88mm as per ISO 7810 standard.
5. Datapage layout of new ePassport will be shared to selected bidder for this contract for their design and development after award. Datapage will have preprinted captions.
6. Datapage is compatible with inkjet printing.
7. The ePassport cover material will be latex saturated cellulose with acrylic base coated. cover will have gold foil hot-stamped on front side.
8. ePassport chip will come with transportation key, key shall be securely stored by new system in HSM using key ceremony process with ePasport vendor and DI&E.
9. This key need to be verified or authenticated by new system before electrical personalization of chip.
10. ePassport supports BAC, SAC and EAC authentication methods as defined in ICAO 9303 documents. New system shall implement all the relevant PKI components needed for electrical personalization and electrical quality check of these authentication methods.
11. ePassport will store data group DG1, DG2 and DG3 data in the chip. New system shall be able to implement the security requirement needed as per ICAO 9303 document and electrical personalization as per Logical Data Structure LDS Ver 1.8 or later based on the latest edition of the specifications for ePassport.

Annexure : 2 - Integration diagram.



Application Enrollment
7
1
4
5
6
Image Capture Studio Application
Image
Document Scan
Personalization
Main DB
8
2
9
Document Scanning
Middleware Application
3
11
Signature Capture
Quality Control System
10
12
Proposed Personalization/PKD/PKI
Travel Document Management System
13
16
15
NPKD
Border Management System
Issuance
14
Border DB