



**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 National e-Passport Public Key
Infrastructure solution including ICAO-PKD
integration and Personalization services for the e-
Passports at the Department of Immigration and
Emigration of Sri Lanka**

IFB No. DIE/PRO/PKI/2026

Employer:

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

Contents

1. Introduction	2
2. Overall, Scope of Work	2
3. Implementation Schedule	2
4. Schedule of Requirements	5
4.1 Public Key Infrastructure (PKI) Requirements (scope A)	5
4.2 MRP / eMRP Personalization Facility Requirements (SCOPE B)	24
5. Minimum Qualifications of Key Professional Staff	59
Annexure I	61
SERVICE LEVEL AGREEMENT (SLA)	

1. Introduction

The Department of Immigration and Emigration (DI&E) in Sri Lanka was established in 1948. DI&E oversees the regulation of the country's border control and manages the movement of individuals into and out of Sri Lanka, including the issuance of passports to Sri Lankan nationals. DI&E intends to procure, install, commission and maintain the electronic Public Key Infrastructure (PKI), the ePassport personalization system, and the associated civil, electrical and mechanical data center development works necessary to support both, in compliance with ICAO Doc 9303 (8th edition) and applicable Government of Sri Lanka standards.

2. Overall, Scope of Work

This Volume covers two distinct scopes of work, each detailed as a self-contained Part and a Consolidated Service Level Agreement (SLA).

Scope 1 — Public Key Infrastructure & Data Centre Extension Development: Design, supply, installation, testing, commissioning and maintenance of the CSCA, DS, CVCA, DVCA, nPKD, KMS and HSM components required for the issuance and verification of e-Passports, Civil, electrical and mechanical works required to establish physically secured CSCA and DS zones within DI&E's existing data center on the 8th Floor, “Suhurupaya”, including dedicated power distribution wiring, environmental controls and access control.

Scope 2 — ePassport Personalization Facility : Design, supply, installation, testing, commissioning, operation and maintenance of the MRP/e MRP passport personalization facility at DI&E, as detailed in Scope 2

Consolidated Service Level Agreement (SLA) applicable to the Scope 1 (PKI, incident-based) and Scope 2 (Personalization, availability-based) scopes for the operational period of the contract.

Bidders shall respond to each Scope's minimum mandatory requirement table independently (Column B: Yes/No; Column C: Remarks/References) using the reference numbering given in that scope. Failure to respond to any requirement in any scope may be treated as non-responsive to that scope.

3. Implementation Schedule

The System shall be implemented in phases as set out below: Data Centre Development, followed by Personalization and Printer Hardware Setup, followed by Public Key Infrastructure Implementation and full System Integration and Commissioning.

S.No	Description / Phase	Delivery Date / From the Date of Commencement (T)
1	Requirement finalization, workshop and final requirement approval, covering all activities.	T + 1 month
2	Phase 1: Design, install, test, commission all required Data Centre Development components (A.8 to A.13) to establish the CSCA and DS zones within the existing data center. Core components are: 1. Civil, electrical and mechanical works for the CSCA zone (physically isolated, air-gapped enclosure). 2. Civil, electrical and mechanical works for the DS zone. 3. Dedicated power distribution wiring and UPS routing from the existing distribution board(s) to the CSCA/DS zones. 4. Access control, CCTV and network segregation for both zones. 5. As-built drawings, completion report and Employer's written approval of the completed zones.	T + 6 months
3	Phase 2: Design, supply, install, test, commission all required Personalization and Printer Hardware components (Scope B) to establish the ePassport personalization facility. Commencement of MRP personalization using full or intermediary set up at employer's premises.	T + 3months
4	Completion of all equipment installation/ integration and the commencement of full operation for personalization of e MRP	T + 6 months
5	Phase 3: Design, install, test, commission all remaining Public Key Infrastructure and system-integration components (Scope A, together with Scope B) required to complete the System. Remaining components are: 1. KMS, HSM. 2. Document Signer. 3. CSCA. 4. CVCA. 5. DVCA. 6. Personalization Solution Manager with data aggregation and data preparation as per Sri Lanka e-Passport requirements. 7. Personalization Station Software to drive, interface with and control the personalization and printing equipment installed under Phase 2. 8. Integration with the three input database systems (Demographic, Photo and Fingerprint). 9. QC with mandatory feature to test Sri Lanka e-Passport personalization. 10. nPKD and integration with ICAO-PKD. 11. All the relevant IT hardware, software, database and 3rd- party licenses for the above components. 12. Sri Lanka CERT security assessment. 13. Trial/test run and User/Operational Acceptance Testing.	T + 7 months

S.No	Description / Phase	Delivery Date / From the Date of Commencement (T)
6	Operational Period. Contractor shall perform PKI support and personalization services as per the SLA stipulated in Part 4 until completion of issuance of the contracted volume (approximately 3.15 million e-Passports and 500,000 MRPs).	T + 7 months onward

PROCUREMENT DOCUMENT - PKI DI&E

4. Schedule of Requirements

4.1 public key infrastructure (PKI) requirements (scope A)

Design, Supply, Customize, integrate, Implement, Test and Commission a e-MRT PKI solution at DIE & Data center extension development

The scope of work under this Scope-A, encompasses the end-to-end design, supply, customization, integration, implementation, testing, commissioning, training and operational handover of an e-MRTD Public Key Infrastructure solution including linkage with ICAO-PKD, for the Department of Immigration and Emigration. The selected Bidder shall be responsible for delivering a complete, secure, resilient and standards-compliant PKI environment capable of supporting Sri Lankan ePassport issuance, border inspection and verification, ICAO-PKD participation, certificate publication, certificate revocation management, trust-store distribution, cryptographic key management, audit logging, reporting and long-term operational sustainability. The solution shall be implemented in accordance with applicable ICAO requirements, accepted information security practices and the operational requirements of the DIE.

Thus, the general scope of work under this component will include the following:

- Confirm the detailed business, technical, security and operational requirements in consultation with DIE stakeholders and prepare the final implementation approach.
- Prepare the solution architecture, detailed design, implementation plan, integration plan, test plan, migration and cutover plan, and project delivery documentation.
- Supply, install, configure and integrate all required servers, network infrastructure, PKI, KMS, HSM, certificate management, trust-store, publication, monitoring and supporting infrastructure components.
- Implement the CSCA, Document Signer, Master List Signer, certificate publication, certificate revocation, national public key directory and ICAO-PKD integration capabilities required for e-MRTD operations.
- Integrate the PKI solution with passport issuance, personalization, border verification and other relevant DIE ICT systems through secure, documented and standards-based interfaces.
- Establish secure key-management procedures, key ceremonies, access controls, approval workflows, audit logging, backup, restoration and disaster-recovery arrangements.
- Develop and submit all required operational procedures, administrator guides, configuration documentation, security documentation, training materials and handover deliverables.
- Conduct configuration verification, functional testing, security testing, interoperability testing, user acceptance testing, commissioning and operational readiness verification.
- Provide training, knowledge transfer, warranty support, maintenance support and post-implementation assistance to enable sustainable operation by the DIE.

- The Bidder shall design, supply, install, test and commission the civil, electrical, mechanical, access control and surveillance infrastructure described below — comprising site preparation and physical partitioning of the CSCA and DS zones, dedicated power distribution and UPS routing, and access control and CCTV surveillance systems — in order to upgrade and fit out the Department's existing data Centre to host the PKI infrastructure under Scope A, without disrupting existing data Centre systems and services outside the allocated zones.

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.1	Scope of work		
A.1.1	The selected Bidder is required to design the Public Key Infrastructure (PKI) solution including, all hardware, software, security, workflow and procedural solution to support issuance and verification of e-MRTDs complying with ICAO guidelines and administrative requirements of the DIE. The scope of work in this context should include designing, supply, customizing, implementing, testing, and commissioning of the PKI related components.		
A.1.2	All components of the Public Key Infrastructure — namely the Country Signing Certification Authority (CSCA), Document Signer (DS), Country Verifying Certification Authority (CVCA), Document Verifying Certification Authority (DVCA), national Public Key Directory (nPKD, including its interface to the ICAO Public Key Directory), Key Management System (KMS), and Hardware Security Module (HSM) — shall be designed, supplied, installed, and commissioned by the successful Bidder as part of this Contract.		
A.1.3	The solution shall comply with ICAO Doc 9303 Parts 1, 2, 3, 4, 9, 10, 11 and 12, including the 2021 eighth edition requirements for Public Key Infrastructure for MRTDs. The solution shall also support ICAO PKD operational procedures for automated exchange of Document Signer Certificates, Certificate Revocation Lists and Master Lists. These functions should be available at all DIE operational endpoints, through integration with existing ICT system where applicable. The integrations shall be based on secure REST-APIs.		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.1.4	The scope of work shall include the design and implementation of the national public key directory (nPKD) for the DIE operations and integration with the ICAO-PKD for operational purposes.		
A.1.5	The proposed solution shall support the issuance of Extended Access Control (EAC) certificates for e-Passports in accordance with Logical Data Structure 1 (LDS1). At a minimum, the proposed solution shall include the following modules, each of which shall comply with the latest release of BSI TR-03110 and ICAO Doc 9303 (8th Edition): a. Country Verifying Certification Authority (CVCA); b. Document Verifying Certification Authority (DVCA); and c. Administrative Certification Authority (Admin CA), for officer authentication and machine-to-machine authentication.		
A.1.6	The CVCA, CVCA link, DVCA and IS certificates MUST be in a verifiable format a. The solution shall support CVCA key rollover. b. The solution should be able to sign DV and IS certificate requests c. The solution should support authorizations for certificate holders as CVCA, DV, IS with read access rights to DG3 (Fingerprint).		
A.2	Functional Requirements-PKI solution general		
A.2.1	The proposed PKI solution must follow and comply with the guidelines/requirements stated in the following ICAO documents. a. ICAO Doc 9303 (Parts 1 to 12 as applicable) including the 2021 eighth edition requirements relating to PKI for MRTD) b. ICAO Public Key Directory (PKD) Regulations c. ICAO PKD Procedures Manual d. ICAO PKD Technical Interface Specification (TIS) e. Any specific requirement included in the ICAO-PKD onboarding Memorandum of Understanding (MoU)		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.2.2	The solution shall implement Passive Authentication as a mandatory capability for all Sri Lankan and all foreign eMRTDs inspected at Sri Lankan borders. The solution shall verify the Document Security Object, signed data group hashes, Document Signer Certificate chain, CSCA trust anchor, CRL status, certificate validity period, signature algorithm, and document-chip data integrity before a document is accepted as electronically valid.		
A.2.3	The issuance PKI shall include, at minimum, one national Country Signing Certification Authority for Sri Lanka, one or more Document Signer authorities, one Master List Signer authority, one national certificate and revocation publication service, one ICAO PKD interface service, one Key Management System, certified Hardware Security Modules, offline backup and recovery capability, and administrative workstations for secure PKI operation.		
A.2.4	The border validation solution shall include a national trust-store service for CSCA certificates, Document Signer Certificates, CRLs, Master Lists, deviation lists and defect lists. The service shall distribute validated trust material to all border inspection systems using authenticated, encrypted and auditable mechanisms.		
A.2.5	The selected bidder shall deliver the solution using open standards and documented interfaces. The solution shall not require a proprietary specific HSM brand, specific proprietary chip supplier, specific proprietary personalization machine, specific proprietary passport booklet supplier, proprietary border-control system, country-specific foreign implementation, or vendor-controlled certificate distribution service.		
A.2.6	The supplier shall provide all certificate profiles, CRL profiles, Master List profiles, object identifiers, ASN.1 structures, policy identifiers, algorithm identifiers, transport protocols, interface specifications, certificate rollover procedures, key ceremony scripts, backup procedures, disaster recovery procedures, and operational manuals as project deliverables		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.2.7	The selected bidder shall configure the system so that Sri Lanka can operate the PKI independently after acceptance, including generation, renewal, suspension, revocation, publication, export, import, validation, archival and destruction of all keys, certificates, CRLs and Master Lists without dependence on the supplier's hosted services or personnel.		
A.2.8	The implementation shall include Extended Access Control, Chip Authentication, Terminal Authentication and PACE support for inspection and future passport-profile compatibility. These functions shall comply with ICAO Doc 9303 Part 11 and BSI TR-03110 certificate and protocol profiles where EAC-compatible data groups or terminal authorization are used.		
A.2.9	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).		
A.2.10	The Document Signer shall be agnostic to CSCA (Country Signing Certification Authority).		
A.3	Functional requirements: ICAO-PKD Onboarding and integration		
A.3.1	The selected bidder shall support Sri Lanka in completing ICAO Public Key Directory participant onboarding, including preparation of technical and procedural inputs required for registration, nominated roles, operational contacts, certificate submission arrangements, testing coordination, and transition to active PKD participation.		
A.3.2	The solution shall provide a dedicated ICAO-PKD integration service capable of uploading Sri Lankan Document Signer Certificates, Certificate Revocation Lists, CSCA link certificates where applicable, Master Lists, deviation lists and defect lists through ICAO-approved channels and in formats conformant with ICAO Doc 9303 and PKD interface requirements.		
A.3.3	The solution shall support automated and manual download of ICAO PKD content for passport verification, including		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	Document Signer Certificates, CRLs, CSCA Master Lists, deviation lists, defect lists and other conformant or non-conformant content categories made available by the PKD for validation use.		
A.3.4	The PKD integration service shall validate all outbound objects before upload, including certificate profile, issuer and subject fields, key usage, extended key usage where applicable, algorithm identifiers, validity periods, CRL numbering, Master List signature, country code consistency, ASN.1 encoding and conformance to ICAO PKD schema and naming conventions.		
A.3.5	The solution shall validate all inbound ICAO PKD content before importing it into the national trust store, including signature verification, certificate chain validation, CRL processing, Master List verification, duplicate detection, expiry checks, revocation status, algorithm policy checks, conformance status and source authenticity.		
A.3.6	The selected bidder shall provide procedures for secure submission and management of Sri Lanka CSCA certificates for ICAO PKD and Master List purposes, including out-of-band or diplomatic-channel exchange where required, CSCA rollover handling, link certificate publication and update of national and foreign trust anchors.		
A.3.7	The ICAO-PKD integration shall be fully connected to both the passport issuance environment and the border verification environment. For issuance, it shall publish the certificates and revocation data required for other States to verify Sri Lankan e-Passports. For verification, it shall distribute downloaded and validated PKD trust material to all Sri Lankan border inspection systems.		
A.3.8	The solution shall maintain separate PKD staging, test and production configurations, with controlled promotion of objects from test to production, documented test evidence, rollback capability, approval workflow and clear segregation of duties between preparation, approval and publication functions.		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.3.9	The solution shall provide scheduled PKD synchronization, configurable polling intervals, retry handling, failure alerts, exception queues, manual override controls and complete audit logs for every upload, download, validation, import, rejection, publication and trust-store distribution event.		
A.3.10	The selected bidder shall conduct ICAO-PKD integration testing and acceptance testing covering participant onboarding readiness, upload of Sri Lankan DSCs and CRLs, Master List publication, download and validation of PKD contents, import to the national trust store, distribution to border systems, validation of foreign e-Passports and operational recovery after communication failure.		
A.3.11	The selected bidder shall provide training, operational manuals and runbooks for ICAO-PKD administration, including onboarding support, certificate upload, CRL upload, Master List handling, downloaded-content validation, incident handling, revocation emergency procedures, compliance reporting and coordination with ICAO PKD support channels.		
A.3.12	The solution shall generate operational and compliance reports showing PKD upload status, downloaded-content status, validation failures, expired or soon-to-expire certificates, CRL currency, Master List currency, synchronization history, rejected objects, trust-store distribution status and border-verification readiness.		
A.4	Functional requirements: Certificate sharing with non-ICO-PKD countries		
A.4.1	The solution shall support supplementary certificate-sharing mechanisms for issuing States, territories, authorities or organizations that are not active participants in the ICAO PKD or whose certificate, CRL or Master List content is not available, current or complete through ICAO PKD channels.		
A.4.2	The selected bidder shall implement a bilateral and multilateral certificate exchange workflow for CSCA certificates, CSCA link certificates, Document Signer Certificates, Certificate Revocation Lists, Master Lists,		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	deviation lists, defect lists, fingerprints and associated metadata received from non-PKD sources.		
A.4.3	The solution shall support standard technical interfaces for non-PKD certificate acquisition, including manual import of signed files, secure file transfer, secure email attachment processing, authenticated web download, HTTPS publication portals, LDAP directory retrieval, diplomatic-channel import packages, removable-media import under controlled procedure, and API-based exchange were agreed by the issuing State.		
A.4.4	The solution shall support secure outbound publication of Sri Lankan public certificate material for non-PKD receiving States, including CSCA certificates, CSCA link certificates, Document Signer Certificates, CRLs, Master Lists, deviation lists, defect lists, certificate fingerprints, validity metadata and contact information through approved bilateral channels.		
A.4.5	The selected bidder shall provide procedures for out-of-band trust establishment for CSCA certificates received from non-PKD sources. These procedures shall include verification through diplomatic notes, embassy or consular handover, authorized government contact confirmation, independent fingerprint comparison, comparison against trusted Master Lists, comparison with previous CSCA link certificates, and confirmation against official issuing-authority publication points.		
A.4.6	The system shall enforce configurable trust classifications for non-PKD certificate material, including trusted, provisionally trusted, restricted-use, expired, superseded, revoked, rejected and quarantined states. Imported certificates shall not be distributed to production border systems until the required approval, verification and risk-rating workflow has been completed.		
A.4.7	The solution shall maintain a complete register of non-PKD issuing States and certificate sources, including country code, issuing authority, source channel, responsible official, contact details, certificate type, fingerprint, validity period, verification evidence, last update date, next review date, approval status and associated operational restrictions.		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.4.8	The system shall validate all non-PKD objects before acceptance, including certificate profile conformance, ASN.1 encoding, signature validity, country-code consistency, issuer and subject naming, key usage, algorithm policy, validity period, CRL issuer and number, revocation status, Master List signature validation, duplicate detection and consistency with existing trust-store records.		
A.4.9	The solution shall support publication and consumption of standard certificate package formats, including DER and PEM encoded certificates, CMS signed Master Lists, X.509 CRLs, signed metadata files, manifest files, SHA-256 or stronger fingerprints, detached signatures, and human-readable certificate exchange forms for operational approval.		
A.4.10	The selected bidder shall provide standard operating procedures for bilateral exchange covering request initiation, authority identification, receipt logging, malware screening, file integrity checking, certificate fingerprint verification, legal or diplomatic verification, technical validation, risk classification, approval, import into staging, production publication, periodic review and emergency removal.		
A.4.11	The solution shall support controlled distribution of approved non-PKD trust material to all border inspection systems using the same authenticated, encrypted, auditable and version-controlled trust-store distribution mechanism used for ICAO PKD data.		
A.4.12	The solution shall provide monitoring and alerts for non-PKD certificates and CRLs, including upcoming CSCA expiry, missing link certificates, stale CRLs, unresolved verification evidence, expired bilateral contacts, failed downloads, failed integrity checks, inconsistent fingerprints, duplicate certificates and certificates requiring periodic revalidation.		
A.4.13	The selected bidder shall provide test cases demonstrating import and validation of non-PKD CSCA certificates through at least three mechanisms: diplomatic or manual handover, secure website or HTTPS download, and LDAP or directory-based retrieval. Testing shall also demonstrate rejection of		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	unverified, malformed, expired, revoked or inconsistent certificate material.		
A.4.14	The solution shall generate reports showing the coverage of ICAO PKD and non-PKD trust material by issuing State, including trust status, source channel, last verification date, CRL currency, Master List availability, operational restrictions, documents successfully validated and cases referred to manual or secondary inspection because trust material was unavailable or incomplete.		
A.5	Functional requirements: Cryptographic Algorithms and Key Requirements		
A.5.1	CSCA keys shall use RSA 4096 with SHA-384 or SHA-512, or ECC P-384 with SHA-384. RSA 2048 shall not be used for new CSCA keys.		
A.5.2	Document Signer keys shall use RSA 3072 or RSA 4096 with SHA-256 or stronger, or ECC P-256/P-384 with SHA-256/SHA-384. The final algorithm set shall be configured consistently across personalization, EF.SOD generation and border validation.		
A.5.3	Master List Signer keys shall use RSA 3072 or stronger, or ECC P-256/P-384 or stronger, with SHA-256 or stronger.		
A.5.4	PACE shall support AES-128, AES-192 and AES-256. BAC shall be supported only for inspection compatibility with legacy foreign e-Passports and shall not be the primary access-control mechanism for newly issued Sri Lankan e-Passports.		
A.5.5	3DES, DES-MAC, SHA-1 and SHA-224 shall not be used for newly generated Sri Lankan certificates, signatures, document security objects, CRLs or master lists.		
A.5.6	All private keys shall be generated, stored, backed up, activated, used and destroyed inside certified HSMs. Plaintext private keys shall never be exported, displayed, logged, stored in a database, or available to any operator, administrator, selected bidder employee or support engineer.		
A.5.7	The proposed HSM shall be at least FIPS 140-3 Level 3 validated or Common Criteria EAL4+ certified		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.5.8	The KMS shall provide full lifecycle management for CSCA, Document Signer, Master List Signer, CVCA, DVCA and Inspection System keys, including generation, activation, suspension, renewal, rollover, revocation, archival, backup, restoration and destruction.		
A.5.9	The KMS shall enforce role-based access control, named-user accountability, multi-factor administrator authentication, dual control for sensitive operations, split knowledge for key ceremonies, four-eyes approval for certificate issuance and revocation, and least-privilege access for all operational roles.		
A.5.10	The KMS and HSM environment shall support documented key ceremonies for CSCA creation, Document Signer creation, Master List Signer creation, certificate rollover, CRL signing, HSM backup, HSM restoration, disaster recovery, key destruction and emergency revocation.		
A.5.11	The solution shall maintain tamper-evident audit logs for all PKI, KMS, HSM, certificate, CRL, Master List, trust-store, administrator and system events. Audit logs shall include timestamp, operator identity, source system, action performed, object affected, result, approval workflow and cryptographic verification status.		
A.5.12	The solution shall use a trusted time source for certificate validity, CRL issuance, audit logging and validation decisions. Time synchronization failures shall raise alerts and shall be handled according to a documented operational procedure.		
A.5.13	The system shall generate CSCA certificates, Document Signer Certificates, Master Lists and CRLs in formats compatible with ICAO Doc 9303 and ICAO PKD processing. The system shall validate all objects before publication or upload.		
A.5.14	The system shall generate CSCA certificates, Document Signer Certificates, Master Lists and CRLs in formats compatible with ICAO Doc 9303 and ICAO PKD processing. The system shall validate all objects before publication or upload.		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.5.15	The solution shall support automated download and import of ICAO PKD data, validation of ICAO Master Lists, manual and automated import of bilaterally exchanged CSCA certificates, and publication of Sri Lankan Document Signer Certificates, CRLs and Master Lists through the approved national and ICAO PKD channels		
A.5.16	The selected bidder shall provide interoperability testing with sample e-Passports and certificate material from at least ten ICAO-compliant issuing States, including Asian, European and Middle Eastern issuers, and shall demonstrate successful validation using Sri Lankan border-inspection systems.		
A.5.17	The selected bidder shall provide acceptance tests covering CSCA creation, DS creation, EF.SOD signing, passport personalization integration, CRL issuance, Master List signing, ICAO PKD upload/download workflow, border trust-store update, passive authentication, PACE, chip authentication, terminal authentication, revocation checking, disaster recovery and audit-log review.		
A.5.18	The solution shall include a documented migration and rollover plan for future algorithm upgrades, CSCA renewal, DS certificate rotation, HSM replacement, data-Centre migration, border-system expansion and integration with future Digital Travel Credential or LDS2 capabilities.		
A.5.19	The proposed 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.		
A.5.20	The KMS (Key Management System) 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.		
A.6	Training and knowledge transfer		
A.6.1	Comprehensive training sessions shall be provided for system administrators, technical support staff, and end users, covering system installation, operational procedures, maintenance activities, and troubleshooting techniques		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.6.2	Knowledge transfer shall include detailed documentation on system architecture, configuration, certificate management, disaster recovery protocols, and security controls, ensuring continuity and self-sufficiency post-deployment.		
A.6.3	Hands-on workshops and practical demonstrations shall be conducted to familiarize staff with key workflows, such as certificate issuance, validation, PKD data handling, and audit log review.		
A.6.4	Ongoing support and refresher training opportunities shall be available to address system updates, patch updates, migrations, and integration with future technologies or system enhancements.		
A.7	Non-Functional requirements		
A.7.1	The hardware infrastructure supporting the solution shall utilize enterprise-grade servers installed within the DIE's existing server room, leveraging current network connectivity and baseline security controls such as firewalls and VPN connections.		
A.7.2	The purchaser will provide the following infrastructure components: a) Floor space within the DIE serve room for a single (44U) server rack. b) 230VAC, 50Hz, 3Ph un-interrupted power from the DIE central UPS solution (shared with other server infrastructure). Power will be available from Server room UPS DB. c) Two ports from the DIE core fiber network (including LAN and Internet access) Apart from the above, all other components, modules, accessories, etc. must be provided by the selected Bidder.		
A.7.3	All interfaces with the DIE ICT systems (including the personalization system interface) must be made through standard, secure REST-api endpoints published and subscribed by the relevant service modules.		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.7.4	All central hardware components should be provided with dual network interfaces and dual power supplies for redundancy		
A.7.5	All equipment supplied under the contract shall include a comprehensive, onsite warranty period of not less than 3 years. The warranty shall include/cover the following conditions. a) The warranty shall commence from the date of commissioning the system for live operations. b) Any critical failed component that stores sensitive information (storage, HSM, etc.) will be retained by the DIE in case of the replacement (non -returnable components)		
A.7.6	The solution must be supported with an annual maintenance support agreement, starting from the end last date of the warranty. The Bidder must include a draft of the proposed annual maintenance agreement with the Bid.		
A.7.7	The selected Bidder will be required to sign a service level agreement covering all critical services and components in the solution. A draft version of the service level agreement must be included in the Bidding document.		
A.7.8	The Bidders shall provide a draft copy of the standard warranty agreement, included in the Bidding document.		
A.7.9	All active equipment (servers, storage, HSM, etc.) but have a published end-of- life greater than 5 years and end-of-support for over 10 years from the date of Bid document submission. The Bidder's must include necessary documentation from the OEM suppliers to prove the end-of -life and end of support life.		
A.7.10	All licenses applicable to the system components shall be provided on a perpetual basis and shall remain valid for use across all DIE operational locations. The licenses shall not be restricted by number of users, seats, transactions, documents, certificate volumes, inspection volumes, issuance volumes, or any other usage-based limitation.		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.7.11	All components provided for the system shall have their ownership/subscriptions registered with eth respective OEM suppliers on the DIE's title.		
A.7.12	The title ownership of all equipment/components/modules provided under this Scope must rest with the DIE from trek date of final acceptance.		
A.8	PKI System Continuity of the system and Handover mechanism		
A.8.1	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 licenses applicable should be able to renewed by employer independently on contract completion		
A.8.2	Documentation Submission The following updated and finalized documents must be submitted: a. PKI System Architecture Diagram (latest version with all changes incorporated) b. Implementation Diagram (detailing the setup, connections, and security layers) c. PKI Policies and Procedures (Certificate Policy (CP) and Certification Practice Statement (CPS)) d. Installation, Configuration, and Administration Manuals e. Security and Compliance Reports f. Any applicable disaster recovery and business continuity plans		
A.9	Documentation Requirements		
A.9.1	The selected Bidder shall design, deploy, configure, and document the physical infrastructure for the Country Signing Certification Authority (CSCA) and Document Signer (DS) environments to be established within the Department's existing data Centre on the 8th Floor, "Suhurupaya", in full		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	compliance with ICAO Doc 9303 Part 12 (Public Key Infrastructure for MRTDs) and applicable Government of Sri Lanka physical security standards.		
A.9.2	The Bidder shall deliver comprehensive documentation covering the operational policies and procedures applicable to the CSCA and DS zones, including access control procedures, environmental monitoring procedures, physical-security incident response procedures, and maintenance procedures for all installed civil, electrical, and mechanical systems.		
A.9.3	The Bidder shall submit as-built drawings, audit trails, and a signed completion report confirming that the civil, electrical, and mechanical works were executed in full accordance with the Employer-approved design and ICAO Doc 9303 Part 12 requirements, prior to handover of the zones.		
A.10	Site and Zone Architecture		
A.10.1	The Employer will provide the designated space within the existing 8th Floor data Centre at "Suhurupaya" for the CSCA and DS infrastructure. The exact allocated area shall be confirmed by the Employer at contract commencement.		
A.10.2	The Bidder shall design and construct two separate, physically secured zones within the allocated space: (a) a CSCA zone, built as a physically isolated, air-gapped enclosure suitable for strictly offline operation of the CSCA root servers and Hardware Security Modules (HSMs); and (b) a DS zone, separately secured and access-controlled, to host the operational DS servers, HSMs, and associated issuing infrastructure.		
A.10.3	Both zones shall be enclosed by secure physical partitions or cages that are strictly segregated from each other and from any other infrastructure within the existing data Centre, meeting ICAO physical security and key-protection guidelines.		
A.10.4	The Bidder shall not modify, relocate, or interfere with any existing data Centre infrastructure, equipment, cabling, or services located outside the allocated CSCA/DS zones without the Employer's prior written approval.		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.11	Power Infrastructure and Distribution Wiring		
A.11.1	The Bidder shall assess the capacity and condition of the nearest existing power distribution board(s) (DB) within the data Centre and shall design, supply, and install dedicated power wiring/circuits from the identified DB(s) to the CSCA and DS zones, sized to the actual connected load of all proposed equipment plus a minimum of 25% spare capacity.		
A.11.2	Where the existing DB(s) do not have sufficient spare capacity or protective device rating for the additional load, the Bidder shall propose and, upon the Employer's approval, supply and install any necessary DB upgrades, additional protective devices/ways, or a new sub-distribution board dedicated to the CSCA/DS zones.		
A.11.3	Power wiring from the DB to each zone shall be provided as dual, physically separated paths wherever the existing DB configuration supports an A-feed/B-feed (dual-corded) arrangement, so as to eliminate single points of failure between the DB and the zone's power distribution units (PDUs)/rack PDUs.		
A.11.4	All power circuits serving the CSCA and DS zones shall be routed through the data centre's existing Uninterruptible Power Supply (UPS) system, or a zone-dedicated UPS supplied by the Bidder where the existing UPS lacks spare capacity. The Bidder shall confirm and document, in writing, the available UPS backup capacity and runtime for the added load.		
A.11.5	All cabling shall be installed in dedicated, labelled containment (trunking/conduit/cable tray), physically separated from data cabling where required by applicable electrical code, terminated with clear circuit labelling at both the DB end and the zone end, and accompanied by an updated single-line diagram and load schedule submitted to the Employer.		
A.11.6	The Bidder shall submit a power load calculation for the CSCA and DS zones, itemising HSM, server, network, and auxiliary loads, as part of the submittals required under C.6, and shall carry out load testing and certification of the		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	completed power installation prior to handover, with results documented in a commissioning report.		
A.11.7	All electrical installation work shall comply with applicable Sri Lankan electrical codes and Ceylon Electricity Board (CEB) requirements, and shall be certified by a licensed electrical contractor/engineer, with certification submitted to the Employer prior to energisation of any CSCA/DS equipment.		
A.12	Access Control, Surveillance, and Network Segregation		
A.12.1	The Bidder shall design, supply, install, and commission multi-factor physical access control systems for both the CSCA and DS zones, with access logs retained for a minimum of 180 days and made available to the Employer on request.		
A.12.2	The Bidder shall design, supply, install, and commission dedicated CCTV surveillance covering all entry points, equipment areas, and cage/partition boundaries of both zones, with footage retained for a minimum of 180 days.		
A.12.3	The Bidder shall design and install secure, segregated network cabling infrastructure for the CSCA and DS zones, physically and/or logically separated from the general data centre network, conforming to ICAO PKI boundary requirements.		
A.12.4	The Bidder shall supply and install equipment racks and lockable server cabinets within both zones suitable for the proposed HSM and server equipment, including cable management and labelling consistent with the Employer's existing data centre standards.		
A.13	Submittals and Approvals		
A.13.1	Prior to commencement of any installation work, the Bidder shall submit the following for the Employer's review and written approval: (a) proposed architectural floor layout and equipment placement plan for both zones; (b) physical partition/cage design and material specifications; (c) power load calculations, single-line diagram, and cooling distribution plan (per C.3 and C.4); and (d) access control and CCTV system design.		

	Column A	Column B	Column C
Ref No.	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
A.13.2	No civil, electrical, or mechanical work shall commence within the existing data centre until the Employer has provided written approval of the submittals in C.6.1, and all such work shall be scheduled and coordinated with the Employer so as not to disrupt the operation of existing data centre systems and services located outside the allocated CSCA/DS zones.		
A.13.3	Key Generation & Ceremonies: Selected bidder shall Execute or provide complete technical support for the CSCA and DS key generation and certificate issuance ceremonies including KGC script.		

PROCUREMENT DOCUMENT - PKI DI&E

4.2 MRP /eMRP Personalization Facility Requirements (Scope B)

Scope B: Design, Supply, Install, Test, Commission and Maintain MRP/eMRP personalization facility at the DIE.

The scope of work for the Scope B includes the design, supply, installation, testing, commissioning, technical operation, and maintenance of an MRP/eMRP passport personalization facility at the Department of Immigration and Emigration. The selected Bidder shall provide a complete end-to-end solution comprising the required personalization equipment, ICT systems, software, security controls, operational support, consumables, maintenance services, training, integration with DIE systems, quality assurance and quality control arrangements, stock and inventory management functions, reporting and audit capabilities, and service-level commitments. The facility shall be capable of securely receiving personalization data from the DIE, personalizing both visible passport data and ePassport chip data in accordance with applicable ICAO and national requirements, verifying the completed passports, handing them back to the DIE for acceptance and dispatch, and maintaining the required throughput, reliability, security, compliance, billing, and performance standards throughout the contract period.

The key activities under this scope of work include the following:

- Design, supply, install, test, commission, operate, and maintain the MRP/eMRP passport personalization facility at the DIE premises.
- Provide all required personalization equipment, ICT systems, software, modules, accessories, consumables, technical operational resources, and technical services.
- Integrate the personalization system with the DIE passport enrolment, issuance, verification, inventory, reporting, and audit systems through a data-base back-end interface and secure REST API-based interfaces.
- Receive personalization data from the DIE, assign passport blanks, personalize visible passport data, encode and verify ePassport chip data, and return completed passports and electronic records to the DIE.
- Implement quality assurance and quality control processes covering printed data, MRZ readability, chip functionality, security features, document integrity, and acceptance status.
- Maintain security, access control, CCTV monitoring, data protection, data retention, audit logging, and compliance controls in accordance with applicable legal, ICAO, ISO/IEC, and Government of Sri Lanka requirements.
- Manage daily passport blank stock, damaged or void booklets, reconciliation records, inventory movements, and related reporting functions required for operational control.
- Meet the specified throughput, priority-based turnaround times, redundancy, availability, service-level, billing, penalty, surcharge, and reporting requirements throughout the contract period.
- Provide training related to operational aspects, testing support, site acceptance testing, trial runs, commissioning support, maintenance, corrective actions, and ongoing operational assistance to the DIE.

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
B.1	Scope of work		
B.1.1	The selected Bidder shall design, supply, install, test, commission, operate, and maintain a passport personalization facility at the DIE for the personalization of passport blanks using personalization data provided by the DIE. The facility shall support both Machine-Readable Passport (MRP) personalization and electronic Machine-Readable Passport (eMRP) chip personalization, and shall include all required hardware, software, operational resources, technical services, consumables support, and associated liveware necessary for reliable end-to-end operation.		
B.1.2	The proposed personalization facility shall have the capacity to personalize the current passport stock of approximately 3.15 million e- passports & 500,000 MRP passports. Based on current enrolment statistics, this stock is expected to be completed within 60 months. The personalization volume is expected to consist primarily of e-passports, with a smaller proportion of regular Machine-Readable Passports (MRPs) of a similar type.		
B.1.3	Payments under the personalization contract shall be made under an operational expenditure (OpEx) payment model. Payments shall become due only after the passports have been personalized, handed over to the DIE, and passed the applicable quality assurance and acceptance checks. Payments are expected to be processed on a monthly billing cycle, based on invoices submitted by the selected bidder and verified against the accepted production output for the relevant billing period.		
B.1.4	During the contract period, the selected Bidder shall be fully responsible for ensuring that the personalization facility remains operational and capable of meeting the specified throughput, accuracy, reliability, availability, and quality		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	requirements. The selected Bidder shall be responsible for supplying all consumables required for personalization, other than passport blank booklets, and for providing preventive maintenance, corrective maintenance, technical assistance, spare parts, software support, operational support, and all other related services necessary to maintain the required performance levels. The DIE's operational responsibilities shall be limited to providing passport blank booklets and assigning DIE staff for the agreed operational functions.		
B.1.5	The selected Bidder shall enter into a Service Level Agreement (SLA) with the DIE in relation to the services provided under the contract. The SLA shall define the required service levels, performance standards, operational availability, quality requirements, reporting obligations, and escalation procedures. The SLA shall also specify the penalties or service credits applicable where the Selected bidder fails to maintain the agreed service levels or required quality standards within the relevant billing cycle.		
B.2	Integration with DIE passport issuance system and ICT systems		
B.2.1	In the current configuration, the DIE operates separate but interconnected systems for passport enrolment and passport personalization, with integration currently managed through a shared database backend. The existing passport enrolment system will continue to be used; however, the current passport personalization system will be replaced by the solution proposed under this tender. The enrolment process presently includes the following functions that are directly relevant to the functional scope of this tender: • Capture and validation of the applicant's biographic data.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	• Capture of an ICAO Doc 9303-compliant digital photograph of the applicant, including validation against applicable ICAO requirements for pose, illumination, resolution, image size, and other relevant quality parameters. • Capture of digital fingerprint images from applicants in 10-print format using the 4+4+2 method. At present, fingerprints are used for de-duplication purposes, and the related biometric data are maintained as raw images and template records. • Provision of the data required for passport personalization to the personalization system through a secure integration mechanism. • Receipt of the personalized passport and the associated electronic personalization data record from the personalization facility, followed by quality verification of the passport prior to dispatch to the bearer. The proposed personalization facility shall operate between steps (d) and (e) described above. Accordingly, the facility shall electronically receive the data required for passport personalization from the enrolment system. After the passport has been personalized, the facility shall return both the completed passport and the corresponding electronic personalization record to the enrolment system. This record shall include the personalization-specific data attributes required for downstream processing, including, but not limited to, the assigned document number and related production details. The enrolment system will then perform the required quality control checks on the personalized passport before the document is finally dispatched to the bearer. The DIE will update its current enrolment system to support REST API-based integration with the		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	proposed personalization system, replacing the existing database backend integration approach. The selected Bidder shall therefore ensure that the proposed solution is capable of securely interfacing with the DIE enrolment system through REST APIs and of supporting the required data exchange, acknowledgement, status updates, and error-handling processes necessary for uninterrupted passport production operations.		
B.2.2	The ICT systems associated with the proposed personalization facility shall be installed, operated, and maintained as a separate sub-system that is logically separated from, but loosely coupled with, the main DIE ICT system. The two systems shall exchange data through a secure, service-oriented REST API interface. In general, the following data exchanges are expected: a) Transfer of personalization request data records from the DIE main ICT system to the personalization system through a secure service API endpoint published by the personalization system. These records shall contain the required personalization parameters and related production instructions. b) Transfer of data relating to the personalized passport from the personalization system back to the DIE main ICT system through a secure service API endpoint published by the main system. Such data shall include, where applicable, the document number, personalization status, production details, and PKI-related information. c) Exchange and synchronization of data required for monitoring and auditing the passport supply and personalization process, including data required for invoicing,		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	operational monitoring, audit trails, reconciliation, and reporting activities. d) Querying of the status of any passport enrolment record that has been handed over for personalization, including the current personalization status, production progress, exception status, and expected handover time after completion of personalization. The Selected bidder selected under this tender shall work collaboratively with the DIE and the DIE's main ICT systems provider to design, implement, test, commission, and maintain the above data exchanges and the required integration between the two systems.		
B.2.3	The integration between the passport personalization system and the existing enrolment and border management systems shall be implemented through REST APIs. The DIE will make the necessary modifications to the existing systems to publish the required API endpoints using open-standard protocols. All data exchanged through the REST APIs shall comply with applicable open standards relating to communication protocols, data formats, data encoding, authentication, authorization, and encryption. The selected Bidder shall also expose the required service APIs to enable the enrolment system to submit personalization request data records to the personalization system. These API endpoints shall conform to open standards for protocols, data encoding, data protection, and encryption, and shall support secure, reliable, and auditable data exchange between the systems.		
B.3	Passport personalization process		
B.3.1	Personalization of passport blanks shall be carried out at the DIE premises. The selected Bidder shall establish the required infrastructure, facilities,		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	equipment, systems, operational procedures, and related support arrangements at the DIE's premises to implement the passport personalization solution within the scope defined in this document. The DIE will provide empty building space for the selected bidder to install, operate, and maintain the personalization facility. The DIE's responsibility for the establishment and maintenance of the facility shall be limited to the following: • Provision of empty floor space of approximately 1000 square feet. a. Provision of electricity supply from the main commercial grid and the building's backup generator (230V AC, 50Hz, 3-phase at 60A per phase). The selected bidder shall be responsible for providing UPS systems, power protection, distribution arrangements, and any other related electrical infrastructure required for the personalization facility. b. Provision of air conditioning through the building's central air conditioning system. The selected bidder shall be responsible for providing any additional cooling capacity, environmental control, humidity control, or related arrangements required to maintain the operating conditions specified by the proposed equipment and systems. c. Provision of perimeter physical security in accordance with the existing building security arrangements. d. Provision of DIE operational staff for passport personalization oversight, monitoring, coordination, and related DIE-side operational activities.		
B.3.2	The functional solution boundary for passport personalization shall be as follows:		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	a. The DIE shall release packs of passport blanks from the secure storage facility to the selected Bidder in quantities sufficient to maintain the required personalization volumes for each operational window. b. The DIE shall provide all biographic and biometric data required for passport personalization in electronic format to the selected bidder through a secure service-oriented API. The DIE passport enrolment system shall push the required data into the selected bidder's system for processing. c. The selected Bidder, using assigned and trained DIE staff, shall personalize each passport, including the data page, endorsements, and chip encoding for e-passports, using the technical services, systems, and equipment provided and maintained by the selected bidder. The selected bidder shall be responsible for training the relevant DIE staff to perform these operations in accordance with the approved procedures. d. The selected Bidder, through assigned DIE staff, shall carry out internal quality control checks on the personalized passports before handover to the DIE for onward processing. e. Upon completion of passport personalization and internal quality control, an electronic notification shall be transmitted back to the DIE system. The personalized passports shall then be handed over physically to the DIE for onward processing. The physical handover process shall include scanning of the MRZ and/or chip data into the DIE system, as applicable. f. Any passport spoiled during the personalization process or rejected during internal quality control shall be handled separately and returned to the DIE for post-audit, subsequent cancellation, and destruction in		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	accordance with the DIE's established operational procedures. g. Once the personalized passports are returned for onward processing, the DIE shall carry out its own quality assurance and integrity checks against the original personalization data provided for personalization. Any deviation, inconsistency, or defect identified during these checks shall result in the relevant passport being treated as void and rejected. Information relating to such rejected passports shall be transmitted electronically to the selected bidder for subsequent re-personalization using a new passport blank, where required. Note: Rejected passports shall not be counted for billing purposes. Payments shall be based only on passports that have successfully passed the applicable quality checks and acceptance procedures.		
B.3.3	Personalization of a passport shall generally include the following components and tasks within the personalization system: a) Selection of the relevant personalization data record and assignment of a corresponding passport blank for personalization. b) Personalization of the passport data page with the required biographic, document, and visual data. c) Personalization of any applicable endorsements, observations, or additional data fields required for the relevant passport type. d) Application or verification of document security features, including personalized security features where applicable.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	e) Encoding, verification, and secure locking of the electronic chip for e-passports, where applicable. f) Quality control of the personalized passport, including verification of the personalized data, document integrity, chip functionality, and applicable security features. g) Electronic update to the DIE's system confirming that passport personalization has been completed and indicating the relevant production and quality control status. h) Physical handover of the personalized passport to the DIE for onward processing, acceptance checks, and dispatch-related activities. i) The MRP personalization solution shall provide a component to aggregate Demographic and Photo data from different existing DI&E system. j) The personalization solution shall be modular and scalable to accommodate higher volumes and enable easy update in the future. k) The personalization solution shall be composed of separate modules of which each of the module handles their own separate tasks. l) The personalization solution shall comply with passport related International and Industry Standard. The bidder must list all International and Industry standards that their personalization solution complies with. m) The personalization solution shall be able to interface with other systems over secure and standard manner n) The personalization solution shall be independent from proposed personalization machine suppliers		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	o) The eMRTD 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. p) The eMRTD 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. q) The eMRTD personalization solution shall be PKI suppliers independent so that future change in PKI system shall be possible to integrate with personalization solution. r) The Personalization solution must implement centralized logging with audit trails for all system and user events. s) No EOL or older libraries: The personalization solution shall be developed and run utilizing the new generation and supported libraries. No end-of-life (EOL) or older framework or libraries are allowed. Bidder shall provide evidence through a static code analysis report by using a trusted tool available in the market. t) API-First Integration: All personalization system modules shall communicate with each other using fully documented APIs without direct database connections or proprietary middleware u) 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. v) The personalization solution shall be developed following a framework of Secure Development Life Cycle process.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	w) The personalization solution shall protect confidentiality of the production data & Database		
B.4	Quality assurance and quality control of personalization		
B.4.1	The selected Bidder shall implement a comprehensive quality assurance and quality control system for the verification of personalized e-Passports. The system shall support both individual passport verification and batch-level verification, and shall record the results of all checks for audit, monitoring, reporting, and operational control purposes. At a minimum, the quality assurance and quality control process shall verify the following functions and attributes: • Manual visual inspection of the passport, including verification of the logo, printing quality, security features, physical condition, and the absence of visible damage or defects. • Compliance of the personalized passport with applicable ICAO standards and specifications. • Verification of chip-encoded electronic data against the printed data and the original personalization record to ensure that the data stored in the chip correspond accurately with the data printed on the e-Passport data page. • The system shall support full verification of ICAO electronic travel document security mechanisms, including BAC, SAC, AA, PA, and EAC, as applicable. This shall include verification of the MRZ and chip-encoded data groups,		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	including the ability to read biometric-related Data Group 3 (DG3) through the EAC protocol where applicable.		
B.4.2	All quality assurance and quality control actions, results, exceptions, and decisions shall be logged in the personalization system and made available to the DIE for review, monitoring, reporting, audit, and reconciliation purposes.		
B.4.3	In addition to the quality control checks implemented at the personalization facility, the DIE will carry out its own internal quality control tests on personalized passports. The selected Bidder shall facilitate the DIE in integrating such test procedures with the relevant stages of the personalization process, including the provision of required data, status information, system access, and operational support.		
B.5	Security and data protection requirements		
B.5.1	The selected Bidder shall install, operate, and maintain a CCTV surveillance system at both the primary and secondary personalization facilities, covering all operational areas, storage areas, access points, and other security-sensitive locations. The CCTV system shall retain video footage for a minimum period of 180 days. The DIE shall be provided with full access to the CCTV system for real-time monitoring, review of historical footage, and post-incident audit purposes. The selected Bidder shall install, operate, and maintain an electronic access control system for all production areas, storage areas, and other restricted areas of the primary and secondary personalization facilities. The system shall maintain complete access logs for all persons entering or leaving such areas. The DIE shall be provided with management-level access to the access control system for monitoring, administration, audit, and reporting purposes.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
B.5.2	All data stored on servers, workstations, and related components of the personalization system shall be protected using industry-standard encryption and endpoint protection mechanisms. The information security solution, associated controls, and related procedures shall be certified or independently assessed by a competent independent agency acceptable to the Government of Sri Lanka.		
B.5.3	No equipment within the personalization facility shall be connected to any external network other than the DIE's authorized network. Where Internet access is required for approved purposes such as product updates, security patches, or vendor support, such access shall be provided only through the DIE's network and in accordance with the DIE's approved security procedures.		
B.5.4	within the personalization facility. Any use of removable storage devices for maintenance, troubleshooting, data transfer, or other approved technical activities shall require prior written permission from the DIE and shall be carried out under the supervision of authorized DIE personnel.		
B.5.5	All bearer-specific data relating to the personalization of a passport, other than approved audit logs, shall be purged from the personalization system storage within three hours of handing over the personalized passport to the DIE. No information that could identify the bearer's biographic or biometric data shall be retained within the personalization system beyond the specified retention window, except where expressly approved by the DIE for audit, legal, or operational purposes.		
B.5.6	Movement of equipment into or out of the personalization facility shall be permitted only with the prior approval of the DIE and under the supervision of authorized DIE personnel. All such		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	movements shall be recorded and retained for audit and security review purposes.		
B.5.7	Operational, technical, and maintenance personnel assigned to the personalization facility may be required to obtain security clearance from the relevant government authorities before being permitted to access restricted areas, systems, or sensitive operational data		
B.5.8	All operations and activities of the personalization facility shall be recorded in appropriate system-level logs and audit trails. The DIE shall be provided with unrestricted access to such logs and audit trails for monitoring, investigation, reporting, reconciliation, and audit purposes		
B.5.9	The selected Bidder shall ensure that every component and operational aspect of the personalization system complies with applicable international standards, including relevant ICAO and ISO/IEC standards, as well as applicable Government of Sri Lanka regulations, guidelines, and security requirements. The system shall be periodically reviewed, audited, and upgraded where necessary to maintain compliance with such requirements, at no additional cost to the Government of Sri Lanka		
B.5.10	The selected bidder shall be responsible for the protection, integrity, availability, and controlled retention of all data, backups, audit trails, and logs maintained within the personalization system. The long-term storage arrangements for logs and audit trails shall be agreed with the DIE. The DIE shall be provided with unrestricted access to all such records, including the tools required to search, retrieve, export, and extract relevant records when required		
B.5.11	All systems related to the personalization facility shall comply with applicable national data protection legislation, including the Personal Data Protection		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	Act No. 9 of 2022 and any other relevant data protection requirements in force during the contract period. Any system, procedural, or operational changes required to maintain compliance with such legislation shall be implemented by the selected bidder at no additional cost to the DIE		
B.5.12	The design and implementation of the personalization facility, personalization software modules, supporting systems, and operational processes shall comply with the provisions of the following legislation, as amended from time to time: • The Electronic Transactions Act No. 19 of 2006. • The Computer Crimes Act No. 24 of 2007. • The Personal Data Protection Act No. 9 of 2022.		
B.5.13	The proposed system shall include all the relevant security components such as Firewall, Backup solution, End Point Protection required to execute personalization of e-Passport securely.		
B.6	Equipment, security and personalization requirements		
B.6.1	The selected Bidder shall provide modern, industry-standard, vendor-neutral passport personalization equipment suitable for the personalization of passport booklets with a non-polycarbonate data page protected by a thin laminate. The proposed equipment shall support high-quality colour personalization of the data page using inkjet, dye-sublimation, or an equivalent proven personalization technology suitable for laminated paper-based or composite passport data pages, without causing deformation, delamination, image bleeding, substrate damage, or reduction of document durability.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
B.6.2	The personalization equipment shall be capable of printing the passport bearer's colour facial image, biographic data, document data, machine-readable zone, and any other required visible personalization elements on the data page in accordance with the approved passport design and applicable ICAO Doc 9303 requirements. The printed output shall be sharp, durable, legible, machine-readable, resistant to normal handling, and compatible with the document laminate and security features.		
B.6.3	The make and model of the proposed personalization equipment shall be proven in live passport personalization environments and shall, at the time of bid submission, be in operational use for passport personalization in at least two countries. The Bidder shall provide documentary evidence confirming such operational use, including the name of the issuing authority or personalization facility, the country of deployment, the scope of use, and the period during which the equipment has been used for passport personalization production.		
B.6.7	The Bidder shall include in its bid a complete list of all proposed equipment, systems, modules, accessories, and major components required for the passport personalization solution. The list shall identify, for each item, the brand name, manufacturer, make, model, version or configuration, country of manufacture where applicable, intended function, and quantity proposed. The Bidder shall also provide official OEM documentation, datasheets, brochures, or equivalent technical evidence confirming the specifications, capabilities, supported standards, operating requirements, and performance parameters of each proposed item.		
B.6.8	The equipment shall support endorsement printing, observation printing, and other required variable data printing on designated inner pages of the passport		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	booklet. Such printing shall be aligned accurately with the approved page layout, shall preserve existing security printing and page features, and shall not damage the booklet structure, stitching, laminate, visa pages, or other security components.		
B.6.9	The proposed equipment shall support ePassport chip personalization, including contactless chip reading, data encoding, data verification, chip locking, and post-personalization validation in accordance with applicable ICAO Doc 9303 logical data structure, security mechanism, and public key infrastructure requirements. The system shall support passive authentication and other applicable eMRTD security mechanisms required by the passport design and issuing authority.		
B.6.10	The equipment shall include all necessary modules and accessories for passport booklet feeding, positioning, page opening, page flattening, data page printing, endorsement page printing, chip encoding, machine-readable zone verification, optical inspection, chip verification, reject handling, audit logging, and secure operator control. The design shall allow safe handling of passport booklets of the approved format without excessive mechanical stress or risk of physical damage.		
B.6.11	The personalization system shall be designed to minimize operator intervention between the main personalization stages, including passport booklet feeding, page positioning, data page printing, security feature personalization or verification, endorsement printing, chip personalization, quality verification, and reject handling. The workflow shall be automated to the maximum practical extent, while allowing controlled operator intervention only where required for exception handling, quality review, maintenance, or approved operational procedures. The Bidding document must include detailed information on the operation of the personalization		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	process and at which stages the manual handling will be required.		
B.6.12	The personalization process shall include automatic and/or operator-assisted verification of printed data, colour facial image quality, MRZ readability, data consistency between the printed data page and chip-encoded data, chip accessibility, and completion of all required security and quality checks before the passport is released for handover to the DIE.		
B.6.13	The proposed solution shall be scalable and configurable to support the required production volumes, operational shifts, redundancy arrangements, consumables management, preventive maintenance, and continuity of operations. The Bidder shall state the nominal and sustained throughput of the proposed equipment, including throughput assumptions for data page printing, endorsement printing, chip encoding, verification, and reject handling.		
B.6.14	The data page personalization equipment shall provide a minimum effective print resolution of 600 dpi for visible data page personalization, including the colour facial image, biographic data, document data, MRZ, and other visible personalization elements. The final printed output shall be sharp, legible, machine-readable, and free from visible banding, bleeding, feathering, broken characters, or registration defects.		
B.6.15	The equipment shall support full-colour facial image printing with at least 24-bit colour reproduction or equivalent colour capability. The system shall support ICC-based or equivalent colour management, colour profile calibration, and repeatable colour control to ensure consistent portrait reproduction without visible colour shift, over-saturation, under-saturation, or loss of facial detail.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
B.6.16	Facial images used for personalization shall be processed and printed without degrading the source image below the quality required for passport issuance and biometric verification. The system shall preserve image sharpness, contrast, tonal range, and facial detail, and shall support standard image formats used for passport enrolment, including JPEG or JPEG 2000, as applicable.		
B.6.17	The MRZ shall be printed using ICAO-compliant OCR-B characters, spacing, alignment, contrast, line positioning, and check-digit formatting. The printed MRZ shall be automatically verified after personalization and shall be readable by standard passport readers without manual adjustment.		
B.6.18	The personalization process shall include a minimum of two personalized security features, consisting of variable data or bearer-linked security elements, selected from the following list or from equivalent alternative features proposed by the Bidder and accepted by the DIE: • UV-printed variable data • IR-printed variable data • Personalized ghost image • Microtext with bearer data • Personalized holographic portrait in laminate • Laser-marked variable data on laminate • Personalized secure overlay elements • Personalized guilloche pattern • Variable encrypted 2D code • Covert forensic marker tied to bearer data The Bidder shall ensure that the proposed personalized security features are fully compatible with the current Sri Lanka passport booklet,		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	including the data page substrate, laminate, security printing, booklet construction, chip inlay, and other existing document security components. The implementation of such features shall not adversely affect document durability, machine readability, chip performance, visual inspection, or downstream passport issuance and border control processes. Bidders may propose alternative personalized security features in addition to, or in place of, the features listed above, provided that such features are suitable for passport personalization and meet the security, durability, interoperability, and operational requirements specified in this document. For any alternative feature proposed, the Bidder shall provide verifiable documentary evidence demonstrating that the feature is in operational use for passport personalization in at least two countries at the time of bid submission.		
B.6.19	The personalization equipment shall maintain accurate print registration against the approved data page and endorsement page layouts. Critical printed elements, including the MRZ, facial image boundary, data fields, and endorsement text, shall be positioned within a practical tolerance of ± 0.5 mm.		
B.6.20	Endorsement, observation, and other inner-page variable data printing shall be performed at a minimum effective resolution of 300 dpi, with 600 dpi preferred where fine text, seals, graphics, or other detailed elements are required. Printed endorsements shall be durable, legible, correctly aligned, and shall not obscure or damage existing security printing.		
B.6.21	All printing, curing, drying, or fixing processes shall be compatible the current passport booklet ("P" Series") issued by DIE. The personalization process shall not cause laminate lifting, delamination, warping, cracking, ink migration, colour bleeding, excessive gloss variation, damage to security features, or reduction of document durability.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	Note: Specifications related to the current passport booklets are attached herewith as Annexure A.		
B.6.22	The chip personalization subsystem shall support contactless chip initialization, data group encoding, chip access control configuration, secure messaging where applicable, chip locking, and verification of the encoded LDS data against the printed data page and the original personalization record. The system shall support applicable eMRTD security mechanisms, including Passive Authentication and other mechanisms required by the DIE.		
B.6.23	The personalization system shall provide automatic and/or operator-assisted quality verification covering print presence, print alignment, colour image quality, text legibility, MRZ readability, chip readability, chip data consistency, security mechanism verification, and overall document condition before acceptance.		
B.6.24	The equipment shall support periodic calibration and validation of print alignment, colour management, print density, MRZ reading, optical inspection devices, chip reader/encoder performance, and other quality-critical functions. Calibration records shall be retained in the system and made available to the DIE for audit and operational review.		
B.6.25	For each personalized passport, the system shall record the personalization result, print verification result, MRZ verification result, chip verification result, operator ID, equipment ID, date and time, production batch reference, acceptance or rejection status, rejection reason where applicable, and complete audit trail required for reconciliation and reporting.		
B.7	Passport stock and inventory management functions		
B.7.1	The selected Bidder's personalization solution shall include inventory and stock management functions for blank passport booklets. The solution shall		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	support both bulk stock management and the management of daily personalization stock issued to the selected Bidder for operational use. At a minimum, the stock management functionality shall include the following: A. Maintain itemized stock records for blank passport booklets, including serial numbers, booklet ranges, packaging unit details, receipt references, and current stock status. B. Maintain records relating to stock receipts, re-ordering thresholds, replenishment requests, delivery batches, acceptance checks, and stock reconciliation. C. Manage the issuance of passport booklet blocks or batches to the personalization facility, including issue date, quantity issued, serial number range, receiving officer, responsible operator, and intended production batch. D. Manage the return, segregation, tracking, and controlled custody of damaged, spoiled, rejected, or void passport booklets until they are processed through the approved post-audit, cancellation, and disposal procedures. E. Maintain real-time stock balances, usage records, stock movement history, exception records, reconciliation reports, audit trails, and management reports required for monitoring and control.		
B.7.2	All functions relating to bulk stock management shall remain under the exclusive control and operation of the DIE. The Selected bidder shall manage only the daily personalization stock functions assigned for operational purposes, while the DIE shall be provided with full access for monitoring, reporting, reconciliation, and audit purposes.		
B.7.3	The passport blank stock management system shall provide a secure service-oriented interface, such as		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	REST APIs or an equivalent open-standard interface, for integration with the DIE's internal passport issuance system where required.		
B.7.4	Inventory Management system shall provide a convenient method on how information of incoming batches of blank booklets can be captured into the system in a hassle-free manner for Inventory purposes.		
B.7.5	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 internal systems if required		
B.7.6	The Inventory Management System shall support Dual Control mechanism for sensitive operations such as stock removal, transfer and reconciliation.		
B.8	Throughput, volume and service level requirements		
B.8.1	The passport personalization facility shall be implemented with full end-to-end redundancy and shall not contain any single point of failure in respect of critical production, personalization, verification, data exchange, storage, or operational control functions. The system shall be capable of maintaining at least 50% of its rated production capacity during scheduled maintenance of any equipment, module, component, or supporting subsystem.		
B.8.2	The rated personalization capacity of the system under normal operating conditions shall not be less than the following: 375 passports per hour.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	3,000 passports per 10-hour shift, operating from 8:00 a.m. to 6:00 p.m.		
B.8.3	The maximum permitted time for personalization (referred to as personalization time) of a single passport, measured from the time the relevant personalization data record is submitted to the personalization system until the personalized passport is returned to the DIE, shall be determined according to the priority level assigned to the data record as follows: - Priority Level 1: within 30 minutes. - Priority Level 2: within 120 minutes. - Priority Level 3: within 3 operating shifts.		
B.8.4	The priority level associated with each passport shall be included in the personalization data record forwarded to the system. Under normal operating conditions, based on a 10-hour shift, the system shall be capable of handling the following daily volumes for each priority category: - Priority Level 1: 50 passports - Priority Level 2: 2000 passports - Priority Level 3: 950 passports		
B.8.5	During normal operations, DIE requests for personalization of passports submitted to the facility will not exceed 375 passports per 60-minute moving window, from the beginning of the daily shift. The DIE will not submit any new personalization requests during the last 2 hours of a normal operating shift.		
B.8.6	Extended operating shifts: The personalization facility should be capable of personalization up to 5,000 passports per 24-hour period in order to support any un-expected demand for passports (e.g.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	during pre-holiday periods etc.). This may require the facility to operate for extended hours. However, no additional charges should be applicable for DIE for such operations. For extended hours of operations (beyond 6.00pm) only priority levels 2 and 3 will be applicable.		
B.8.7	In the event that a personalized passport is found as void (i.e. to be rejected due to quality/technical errors) by the employer's final quality checks, the time window for personalization of a new document should be considered from the point of initially handing over the data record provided that the void notification is made within 60 minutes of handing over. However, the time between handing over the initial void passport to employer and informing the invalid state / re-personalization request back to the Selected bidder shall be excluded from the time window calculation.		
B.8.8	If the void notification is not handed over within 60 minutes, the personalization time window for eh passport will be reset to zero.		
B.8.9	No payment will be made for such void / QC failed passports. However, penalties will be applied as per the details given in this document.		
B.8.10	DIE should be able to change the priority level associated with a personalization data record provided, after it has been forwarded for personalization, provided that the following conditions are satisfied. - Selected bidder has not started the personalization procedure related to the data record - The hourly/daily volume limit of the new priority level has not exceeded by the time the change is made.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	In the event that the priority level is changed, the time window for personalization should re-start from the point where the new priority level is specified.		
B.8.11	The selected bidder must provide an interface to employer that facilitate monitoring of personalization status of individual data record / passport during the personalization, including the expected delivery time for the passport.		
B.8.12	The system must provide necessary reporting and auditing tools / REST-api integration point allowing the DIE to monitor the personalization system throughput and to consider such data for billing and auditing purposes.		
B.8.13	Where all personalization requests submitted during a normal 10-hour operating shift are not completed within that shift, the selected bidder shall complete the remaining requests before the commencement of the next operating shift, without prejudice to any applicable service-level requirements, penalties, or reporting obligations specified in this document.		
B.8.14	Employer shall reserves the right to conduct reliability test/failure resilience test on a periodic basis not less than 30 days.		
B.9	Billing cycles, committed volume, penalties, surcharges and payments		
B.9.1	Daily committed volume: The DIE shall commit to a minimum daily volume of 1,000 passport personalization's per calendar day, to be carried out during the regular 10-hour operating shift, provided that all of the following conditions are satisfied: a. The relevant day is a normal DIE working day, and the DIE has submitted at least one valid passport personalization request to the personalization facility during the shift.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	b. No performance or service-level penalties are applicable to the selected Bidder in respect of the relevant shift. c. The personalization facility remains operational at full contracted capacity throughout the relevant shift, and no scheduled maintenance, planned downtime, or Selected bidder-caused service interruption occurs during the shift. Where the above conditions are met, the DIE shall pay for the committed minimum daily personalization volume, whether or not the actual number of passports personalized during the relevant shift reaches 1,000 passports.		
B.9.2	Penalties: The following service-level and performance-related penalties shall apply to payments due to the selected Bidder where the applicable service requirements are not met. Throughput penalty: The throughput penalty shall be calculated based on delays in the turn-around time for each individual personalization request. For this purpose, turn-around time shall be measured from the time the DIE system first attempts to submit the relevant personalization request to the personalization facility until the time the corresponding personalized passport is scanned into the DIE ICT system after handover. The applicable penalty shall be calculated on a per-passport basis as follows: a. Personalization requests submitted under Priority Levels 1 and 2: • First two hours of delay: 0.25 percentage points per passport. Delay beyond the first two hours: 0.1 percentage points per hour, or part thereof, per passport.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	b.Personalization requests submitted under Priority Level 3: First 24 hours of delay: 1 percentage point per passport. Delay beyond the first 48 hours: 0.5 percentage points per calendar day, or part thereof, per passport. The total daily throughput penalty shall be the aggregate of the applicable percentage-point penalties for all passport personalization tasks delayed during the relevant day or shift. c. . Volume penalty: Applicable where the selected Bidder fails to meet the required shift-based personalization volume specified in this document. The throughput penalty shall be calculated using the following formula: $100 * \frac{P_{total} - P_{completed}}{P_{total}}$ For the purpose of this calculation, the applicable total volume (P_{total}) shall be the lower of the total number of valid personalization requests submitted during the relevant shift and the expected volume applicable for that shift. The completed volume ($P_{completed}$) shall mean the number of passports personalized and returned within the shift. The above penalties shall not apply on days where planned maintenance is carried out, provided that the maintenance has been requested in advance by the selected Bidder and approved by the DIE. Where both a throughput penalty and a volume penalty are applicable for the same day, the applicable daily penalty shall be the higher of the two penalty amounts and shall not be applied cumulatively unless otherwise expressly stated in this document.		
B.9.3	The applicable penalty shall be applied as a percentage deduction from the total daily		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	personalization payment due to the selected Bidder, subject to the following conditions: a. The calculated penalty percentage shall be rounded upward to the nearest whole percentage point. b. The maximum aggregate penalty applicable for any single calendar day shall be capped at 60% of the total daily personalization payment due for that day.		
B.9.4	The selected bidder must maintain complete details and audit trails related to each passport personalization workflow enabling a full audit capability on the turn-around time. The details should include different stages of processing from the receipt of the initial request to the handing over of the personalized passport. This audit trail should be accessible to the employer through a proper interface. The interface should also allow the employer to run queries on individual passports as well as to generate required summary / detailed reports.		
B.9.5	Surcharges: A surcharge shall apply for each passport blank or personalized passport that is spoiled, damaged, rendered unusable, or rejected as a result of any technical, operational, handling, or procedural error attributable to the selected Bidder, the selected bidder, its personnel, equipment, systems, consumables, maintenance activities, or approved subcontractors. The surcharge rate will be Euro 5 or equivalent per damaged passport booklet. There is no upper limit for the surcharges applicable per billing cycle. In the event, the surcharge amount exceeds 60% of the payable invoice amount (after deducting penalties), the balance may be carried forward to the following month.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
B.9.6	Billing cycle: Personalization payments shall be calculated on the basis of each normal operational shift and shall be invoiced and paid on a monthly billing cycle. Each billing cycle shall commence with the first operational shift of the relevant calendar month and shall end with the last operational shift of the same calendar month. The following procedure shall apply to invoice submission, verification, dispute resolution, and payment: The selected Bidder shall submit a detailed monthly statement and the corresponding invoice to the designated DIE recipient on or before the second working day of the following month. The DIE shall review the monthly statement and invoice and shall notify the selected Bidder of any objections, discrepancies, or billing disputes within 10 working days of submission. Where no objection or dispute is raised in respect of the invoice, the DIE shall make payment on or before the 20th working day from the date of invoice submission. Where an objection or dispute is raised, the DIE shall pay the undisputed portion of the invoice by the same date. Any objection, discrepancy, or billing dispute shall be resolved within two calendar months from the invoice date. Any payment due following resolution of the dispute shall be made within 10 working days from the date of resolution.		
B.9.7	The invoice and accompanying statement shall be system-generated and shall include the following details for each operational day: a. Personalization volumes by channel. b. Daily penalty calculations and penalties applied. c. Daily surcharges applied. d. Committed volume, where applicable.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
B.9.8	The raw granular data used to generate the invoice and statement shall be made fully available to the DIE for audit and verification purposes.		
B.10	Training, testing and commissioning		
B.10.1	The Bidder shall provide operational training on the personalization facility for 15 members of the DIE's staff. The training shall cover all relevant operational, monitoring, quality control, exception-handling, and routine support activities, and shall be completed before testing of the new facility begins.		
B.10.2	Once the personalization facility is installed and ready for commissioning, DIE will carry out a site acceptance test before the facility can be commissioned for live operations. The site acceptance test will in general include the following. • A vulnerability assessment and a penetration test (especially related to the ICT systems and infrastructure) carried by an external agency nominated by the employer • A process/workflow audit carried out by the DIE • A trial run involving the personalization of around 10000 passports. The selected bidder must immediately rectify any defects, vulnerabilities discovered during these tests without any cost to the employer. If the tests must be repeated due to any un-resolved issue, the cost of subsequent audits/tests must be handled by the selected bidder. The full post commissioning live operation should be started only after the successful completion of these test procedures.		
B.10.3	The DIE may carry out periodic or random tests on personalized passports and the personalization process. The selected bidder must attend and rectify any shortcoming found in such audits with a period		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	of 45 days from information such findings to the selected bidder.		
B.10.4	System integration with existing ICT system: The selected bidder must extend his fullest support for integration of the proposed e-passports and the personalization workflow with the existing ICT systems of the DIE. The support will also include working with the main ICT systems contractor of the Employer for integration and interoperability of the personalization facility and the passport verification activities.		
B.10.5	Before full commissioning and the start of regular operations, the proposed personalization facility shall undergo a test or trial run covering not less than 10,000 passports or five regular operating shifts, whichever provides the broader operational validation.		
B.10.6	Full commissioning and the first billing cycle shall commence only after the successful completion of the test or trial run without any issue that would have resulted in a penalty, surcharge, or material operational failure if it had occurred during regular production.		
B.10.7	If the initial test or trial run identifies any issue, the selected Bidder shall rectify the issue and may repeat the test or trial run up to two additional times within one calendar month. The DIE reserves the right to terminate the contract, without prejudice to any other rights or remedies available to the DIE, if the selected Bidder fails to successfully complete the test or trial runs within the permitted attempts.		
B.10.8	The DIE shall not make any payment for passports personalized during the test or trial runs.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
B.10.9	Regular operations and billing shall commence only after the successful completion of the required test or trial runs.		
B.11	Implementation timeline:		
B.11.1	The selected Bidder shall commence the test or trial runs of the personalization services within 90 days from the date of contract signing.		
B.11.2	The selected Bidder shall complete full commissioning of the personalization system, including all required infrastructure and supporting facilities, within 120 days from the date of contract signing.		
B.12	General requirements		
B.12.1	Operating environment, environmental protection, and climate control: The Bidder shall assess the operating environment and site conditions, including temperature, humidity, power quality, and any other conditions relevant to the proposed personalization facility. The DIE's responsibility shall be limited to providing the facilities specified in this document. The Bidder may conduct a site visit with the prior approval of the DIE.		
B.12.2	Operational and maintenance costs: The Bidder's quoted price shall include all operational and maintenance costs relating to the personalization facility for the entire contract period, except for the following costs, which shall be paid directly by the DIE: - Electricity charges for consumption from the commercial grid. - Water or other utility charges payable to the relevant utility provider.		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	Salaries, wages, and related incentives payable to DIE personnel assigned to the site.		
B.12.3	The Bidder shall include in its bid a detailed breakdown of the expected operational and maintenance costs, including the cost of major consumables and replacement parts. Failure to provide this information may result in the bid being treated as non-responsive.		
B.12.4	Site work and construction: The Bidder shall be responsible for all civil works, modifications, and fit-out activities required to establish the personalization facility, including partitioning, security enclosures, and any other site preparation works necessary for installation and operation.		
B.13	Post Issuance		
B.13.1	The bidder shall include a backend system / solution in their proposal to remediate security vulnerabilities in the chip operating system and/or applications of electronic passports already issued to and held by citizens, by loading signed OS or security patches onto the chip in the field, without replacing or reissuing the physical passport documents.		
B.13.2	The solution / system shall maintain compliance with evolving cybersecurity, cryptographic algorithm, and regulatory requirements over the lifetime of the electronic passport documents, including support for future operating system, security updates, and cryptographic algorithm		
B.13.3	The solution/ system shall provide secure, user-friendly access for citizens and DIE through standard web browsers available in the market supporting different computer operating systems (Windows, Mac OS, Linux), integrated with existing national electronic identification services (e.g. National Identity Provider) where applicable, and shall not		

	Column A	Column B	Column C
Ref#	Minimum requirement	Bidder's response (Yes/No)	Remarks / References
	require dedicated client software installation on the user's computer		

5. Minimum Qualifications of Key Professional Staff

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

No	Position	No of People	PKI project Implementation (Time commitment)	Total Experience in the Proposed Role /Years	Minimum Qualification
1.	Project Manager	1	Full Time	10	- Bachelor's Degree in a relevant field, together with a proven track record of managing large-scale government IT projects, particularly e-passport or PKI systems. - A recognized project management certification (e.g., PMP, PRINCE2, PMI-ACP®, or equivalent) is preferred, with Scrum certification considered an added advantage.
2.	Solution Architect	1	Full Time	10	- Bachelor's Degree in a relevant field, together with TOGAF certification or an equivalent architecture certification. - Demonstrated experience in designing and implementing PKI solutions, including secure authentication, encryption, and digital signature capabilities for e-passport applications.
3.	PKI Specialist	1	Full Time	06	Bachelor's Degree in a relevant field, together with CISSP certification or an equivalent security certification.

					Demonstrated experience in designing and implementing PKI solutions, including secure authentication, encryption, and digital signature capabilities for e-passport applications.
4.	Security Architect	1	Full Time	10	- Bachelor's Degree in a relevant field, together with CISSP and/or CISM certification. - Extensive experience in designing and implementing security frameworks for government digital systems, including the application of cryptographic standards, secure data transmission protocols, and regulatory compliance requirements for e-passport systems.
5.	System Administrator	1	Full Time	06	Bachelor's Degree in a relevant field.

PROCUREMENT DOCUMENT - SUPPLEMENT

Annexure I

DEPARTMENT OF IMMIGRATION AND EMIGRATION

SERVICE LEVEL AGREEMENT (SLA)

Procurement of National e-Passport Public Key Infrastructure solution including ICAO-PKD integration and Personalization services for the e-Passports at the Department of Immigration and Emigration of Sri Lanka

PROCUREMENT DOCUMENT - PKI DI&E

1. Purpose, Scope, and Administrative Framework

This Service Level Agreement (SLA) defines the operational, performance, support, and financial frameworks governing the delivery of services under the Sri Lankan electronic Machine-Readable Travel Document (e-MRTD) project. The agreement is established between the **Department of Immigration and Emigration of Sri Lanka (hereinafter referred to as 'DIE' or the 'Purchaser')** and the **Contractor** selected to execute the project works. This agreement establishes a legally binding structure to ensure high-security, high-availability operations for both the national cryptographic infrastructure and the passport personalization services.

This SLA spans two separate functional Scopes, representing a multi-vendor or unified operational support model, designed to prevent single-point failures and guarantee operational continuity:

- **Scope A (Public Key Infrastructure):** Encompasses the design, supply, customization, integration, implementation, testing, and 5-year maintenance of Sri Lanka's national Country Signing Certification Authority (CSCA), Document Signer (DS), Country Verifying Certification Authority (CVCA), Document Verifying Certification Authority (DVCA), and national Public Key Directory (nPKD) with automated integration into the global ICAO PKD directory. Support transitions from a 3-year standard warranty to an Annual Maintenance Contract (AMC) framework.
- **Scope B (Personalization & Printers):** Encompasses the operational installation, system integration, high-resolution visual printing, secure contactless chip encoding, quality assurance, blank booklet inventory control, and complete support of the e-Passport personalization facility. Scope B operates under a service-based Operational Expenditure (OpEx) payment model where the Contractor is compensated solely for successfully personalized and verified documents handed over to DIE.

2. Scope A: Public Key Infrastructure Service Levels

The Scope A Contractor warrants that the central PKI infrastructure, including all sub-certification authorities, certified Hardware Security Modules (HSMs), key management systems, and directory replication nodes, shall perform in strict compliance with ICAO Doc 9303 (Parts 1 to 12) guidelines and national security requirements. The operational availability of the core system components shall be assessed against rigorous annual performance standards.

2.1 Annual Performance and System Availability Indicators

System availability shall be monitored continuously and reported monthly. If the annual cumulative availability of any core sub-system drops below the defined thresholds, financial deductions shall be applied as a percentage of the Scope A Contract Price or the annual support fees, calculated on a sliding scale.

Ref	Core PKI Sub-System / Component	Mandatory Target (%)	Financial Deduction Formula
A-1.1	Personalization Solution & Reporting module	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.2	KMS & certified Hardware Security Module (HSM)	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.3	nPKD (Read/Write Interfaces & ICAO PKD Interface)	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.4	Document Signer (DS) / Document Verifying CA (DVCA)	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.5	Quality Control (QC) software & Validation endpoints	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.6	Personalization Software for Workstation clients	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.7	Data Centre Central Hardware (Enterprise Servers, Switches)	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.8	Data Centre Platform Software (OS, DB, Virtualization)	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.9	Information Security Applications (EDR, SIEM Firewalls)	>= 99.50%	0.001% of Contract Price per 0.1% drop below target
A-1.10	CSCA & CVCA (Country Verifying Certification Authority)	>= 95.00%	0.001% of Contract Price per 0.1% drop below target

2.2 Daily Availability and Recovery Time Objective (RTO)

In addition to annual cumulative targets, the Contractor is bound to immediate recovery actions during operational windows. The Recovery Time Objective (RTO) for any central PKI sub-system is set strictly at 20 minutes, with a strict target of Zero Data Loss (Recovery Point Objective - RPO = 0). If the Contractor fails to restore live operations within 20 minutes from the initial fault detection, a 1.0% penalty shall be deducted from the monthly maintenance or project support invoice for every incremental 5-minute delay beyond the RTO limit, until full service is restored.

2.3 Support Escalation & Fault Severity Framework

All software, hardware, and integration faults reported by the DIE or detected by automated central monitoring tools shall be classified into one of the four severity levels. Support response and resolution windows are contractually binding:

Severity Level	Operational Definition & Criteria	Response Target	Resolution Target	SLA Breach Penalty
Severity 1 (Critical)	Complete system outage, loss of critical PKI functionality (e.g., signing certificates, ICAO sync failure), or private key compromise. No workarounds available.	15 Minutes	Immediate continuous 24x7 work until restored	LKR 100,000 deduction per incident window
Severity 2 (High)	Loss of critical system module or performance degradation causing operational delays, but a temporary	30 Minutes	Within 2 Hours	LKR 50,000 deduction per incident window

	workaround exists (e.g., backup HSM failover).			
Severity 3 (Moderate)	Minor software or reporting anomalies, GUI navigation defects, or non-blocking technical queries with minimal impact on live production.	2 Business Days	Within 3 Business Days	LKR 10,000 deduction per business day
Severity 4 (Low)	Documentation errors, minor incorrect behavior, aesthetic issues, or technical feature requests that do not affect active PKI or personalization.	7 Business Days	Next scheduled release or Change Request	Subject to joint project review

2.4 Advanced Technical Support for Key Ceremonies

The Scope A Contractor must provide dedicated technical, cryptographic, and administrative support during DIE's critical key ceremonies, which include the Country Signing Certification Authority (CSCA) creation/replacement (mandated every 3 years), Document Signer (DS) key rollover, Country Verifying CA (CVCA) rollover, HSM backup, restoration, or key destruction. The Contractor shall deliver:

- **Ceremony Runbooks:** Submission of formalized, step-by-step key ceremony scripts and procedures at least 15 business days prior to any ceremony.
- **On-Site Expertise:** Provision of at least two certified cryptographic engineers on-site at DIE premises during the entire rehearsal and live ceremony.
- **Formal Auditing:** Co-signing of ceremony logs and providing verification signatures confirming HSM security state, dual-control validity, and split-knowledge compliance.

2.5 Transitional Handover & Exit Criteria

To ensure absolute operational self-sufficiency for DIE and avoid vendor lock-in, the Contractor is bound by strict exit criteria. All PKI-related data—including certificate authorities (CAs), public keys, configuration files, access controls, audit logs, and system database schemas—must be safely duplicated and transferred to a designated DIE server node or nominated third party at least three (3) months prior to the end of the contract period. All perpetual licenses must remain fully active and transferable to DIE without any additional operational charge. A joint audit by Sri Lanka CERT must certify that DIE can operate the system 100% independently post-contract completion.

- **Handover Documentation Deliverables:** As part of the transitional handover, the Contractor shall submit updated and finalized documentation to DIE, including: (a) PKI System Architecture Diagram (latest version, all changes incorporated); (b) Implementation Diagram detailing setup, connections and security layers; (c) PKI Policies and Procedures (Certificate Policy and Certification Practice Statement); (d) Installation, Configuration and Administration Manuals; (e) Security and Compliance Reports; and (f) Disaster Recovery and Business Continuity Plans. [Ref: ScopeA A.8.2]

2.6 Redundancy and No Single Point of Failure (Central PKI Infrastructure)

All central PKI hardware components (CSCA, DS, CVCA, DVCA, KMS, HSM, nPKD and associated servers) shall be provided with dual network interfaces and dual power supplies, and the Contractor shall ensure no single point of failure exists in the central PKI infrastructure that could compromise the availability and RTO targets set out in Sections 2.1 and 2.2 above. [Ref: Scope A A.7.4]

2.7 Technology Currency and Obsolescence Protection

All active equipment supplied under Scope A (servers, storage, HSM, etc.) shall carry a manufacturer-published end-of-life of not less than 5 years and end-of-support of not less than 10 years from the date of Bid submission, evidenced by OEM documentation. The Contractor shall give DIE reasonable advance written notice of any component approaching end-of-life or end-of-support and shall propose a replacement or upgrade path that does not degrade the SLA targets in this Section. [Ref: Scope A A.7.9]

2.8 On-Site Engineering Staffing and On-Call Coverage (Scope A - PKI)

The Contractor shall keep a qualified PKI/HSM/KMS engineer physically present at the DIE premises throughout DIE's normal business hours (8:00 a.m. to 6:00 p.m., Monday to Friday, excluding public holidays) for the duration of the warranty and the subsequent Annual Maintenance Contract period, to support day-to-day PKI operations, fault response, and the key-ceremony support described in Section 2.4.

- **On-Call Responsibility Outside Business Hours:** It shall be the Contractor's sole responsibility, at its own cost, to maintain a documented on-call roster of suitably qualified PKI/cryptographic engineers available outside DIE's normal business hours (evenings, weekends and public holidays), so that the response and resolution targets in Sections 2.2 and 2.3 - including the 15-minute response target for Critical-severity faults - continue to be met at all times, regardless of the hour at which a fault occurs.
- **Roster & Escalation Contacts:** The Contractor shall furnish DIE, prior to commissioning and whenever updated, with the current on-site duty roster and an out-of-hours escalation contact list (names, roles, and direct contact numbers) for the on-call engineers, so that DIE can invoke the fault-severity escalation process in Section 2.3 at any hour.

PROCUREMENT DOCUMENT - PKI DIE

3. Scope B: Personalization & Printer Service Levels

Scope B governs the technical operations and comprehensive maintenance of the passport personalization facility located at DIE premises. All activities operate under a service-based Operational Expenditure (OpEx) payment model where the Contractor provides all consumables (except passport blank booklets), high-security equipment, integration software, onsite engineering resources, and maintenance. Compensation is strictly tied to successful output quality and throughput speed.

3.1 Personalization Facility & Throughput Capacity Targets

The personalization facility must maintain a robust and redundant hardware/software configuration to prevent single-point failures. The facility is contractually bound to the following sustained throughput capacities:

- **Nominal Hourly Throughput:** Minimum personalization rate of 375 passports per hour under normal operating conditions.
- **Sustained Shift Capacity:** Personalization of 3,000 passports per standard 10-hour operating shift (operating from 8
- **Extended Operating Shift:** The Contractor must scale production to personalize up to 5,000 passports per 24-hour period to handle seasonal or peak demands. DIE shall not pay any additional operational fees or hourly surcharges to the Contractor for extended hours or overnight shifts.
- **Redundancy & Maintenance Capacity:** The personalization facility shall be implemented with full end-to-end redundancy and shall contain no single point of failure across production, personalization, verification, data exchange, storage or operational-control functions. During scheduled and DIE-approved maintenance of any equipment, module or subsystem, the Contractor shall maintain no less than 50% of rated production capacity. [Ref: Scope B, B.8.1]

3.2 Priority-Based Turnaround Times (SLA Windows)

Each personalization request transmitted to the personalization system by DIE main ICT systems shall carry an associated priority level. The maximum permitted turn-around time—measured from the moment DIE pushes the biographic/biometric data record to the personalization system API until the completed physical passport is scanned back into the DIE system—is defined as follows:

- **Priority Reassignment:** DIE may change the priority level of a data record after submission, provided the Contractor has not yet begun personalizing that record and the new priority level's hourly/daily volume limit has not been exceeded; the turnaround-time window restarts from the point the new priority level is applied. [Ref: Scope B B.8.10]
- **Shift Overflow Completion:** Where requests submitted during a shift are not completed within that shift, the Contractor shall complete the outstanding requests before the start of the next operating shift, without prejudice to the penalties and SLA obligations in Section 3.6. [Ref: Scope B B.8.13]

Priority Level	Turnaround Time (SLA Window)	Maximum Permitted Daily Volume	Extended Shifts Applicability
Priority Level 1 (Urgent)	Within 30 Minutes	Up to 50 Passports per Day	Fully applicable during extended shifts
Priority Level 2 (Standard)	Within 120 Minutes	Up to 2,000 Passports per Day	Fully applicable during extended shifts
Priority Level 3 (Bulk)	Within 3 Operating Shifts	Up to 950 Passports per Day	Fully applicable during extended shifts

3.3 Quality Assurance & Void Booklet Protocol

In strict compliance with high-security manufacturing principles, any passport booklet spoiled during printing/encoding or found defective by DIE's final QA/QC verification shall be handled as follows:

- **Excluded from Billing:** Spoiled or rejected booklets shall be treated as void and are excluded from billing calculations. DIE shall pay zero fees for un-accepted passports.
- **SLA Time Window Impact:** If a booklet is found void and reported to the Contractor within 60 minutes of physical handover, the re-personalization turnaround time window is measured from the initial handover (excluding the time between physical handover of the void document and the notification of invalid state). If the void notification occurs after 60 minutes, the turnaround window resets to zero.
- **Physical Security Punching (SLA IMPROVEMENT):** All void booklets must be immediately physically punched through the contact/contactless chip and the MRZ area under the direct supervision of DIE staff, logged in the inventory management system under dual-control, and stored in a secure, dual-locked bin for subsequent audited destruction.

3.4 Daily Committed Volumes & Financial Protections

To ensure commercial viability for the Contractor while protecting DIE's fiscal interests, a daily commitment model is established. DIE commits to a minimum daily billing volume of 1,000 passport personalizations per calendar day during normal operating shifts, provided that *all* of the following conditions are simultaneously met:

- Normal working day and DIE has submitted at least one (1) valid passport personalization request during the shift.
- No performance, speed, or service-level penalties are applicable to the Contractor in respect of the relevant shift.
- The personalization facility remains fully operational at 100% contracted capacity throughout the shift, with no scheduled maintenance, planned downtime, or Contractor-caused service interruptions.

Where these conditions are met, DIE shall compensate the Contractor for the minimum committed volume of 1,000 personalizations, regardless of whether actual personalized volume was lower. If any of the above conditions are violated, billing is calculated strictly on actual accepted production output.

3.5 Consumables Supply Chain SLA

To mitigate the risk of stock-outs or defective print batches that could paralyze national passport issuance, the Contractor is bound by a strict consumables supply agreement:

- **Mandatory On-Site Reserve:** The Contractor must maintain an active, on-site storage reserve containing a rolling 3-month supply of all OEM-recommended consumables (including high-security inks, specialized laminates, printer cleaning cartridges, and printheads).
- **Quality Validation:** All consumables must be OEM-certified and pre-tested in the staging environment. Any use of non-compatible or un-authorized consumables shall trigger immediate contractual default.
- **Stock Out Penalty:** If passport personalization is delayed or suspended due to a shortage of consumables, a penalty of LKR 250,000 per shift shall be applied as a deduction, and all throughput penalties shall apply cumulatively.

3.6 Scope B Penalties, Surcharges & Payment Adjustments

Failure to meet turnaround speed, shift volume targets, or secure handling guidelines shall result in financial penalties and surcharges deducted as stipulated in SCOPE 2 — MRP / eMRP PERSONALIZATION FACILITY REQUIREMENTS (SCOPE B) directly from the monthly Operational Expenditure (OpEx) invoice:

3.7 Monitoring, Reporting and Audit Interfaces

The Contractor shall provide DIE the following monitoring, reporting and audit capabilities in respect of Scope B operations:

- **Real-Time Status Monitoring:** A monitoring interface showing the personalization status of each individual data record/passport, including the expected delivery time. [Ref: Scope B B.8.11]
- **Throughput Reporting & API Access:** Reporting/auditing tools and a REST-API integration point enabling DIE to monitor personalization throughput for billing and audit purposes. [Ref: Scope B B.8.12]
- **Turnaround Audit Trail:** Complete audit trails of every processing stage for each passport (from receipt of request to handover), accessible to DIE through a query interface supporting both individual passport lookups and summary/detailed reporting. [Ref: Scope B B.9.4]
- **Raw Billing Data Access:** The raw granular data underlying each invoice and monthly statement shall be made fully available to DIE for audit and verification. [Ref: Scope B B.9.9]
- **Invoice Content Standard:** Each monthly invoice/statement shall be system-generated and include, at minimum: personalization volumes by channel; daily penalty calculations and penalties applied; daily surcharges applied; and committed-volume performance. [Ref: Scope B B.9.8]

3.8 Ongoing Audit Rectification Commitment

Where DIE's periodic or random audits of personalized passports or the personalization process identify any shortcoming, the Contractor shall attend to and rectify the finding within 45 days of the finding being communicated to the Contractor. [Ref: Scope B B.10.3]

3.9 Right to Periodic Reliability and Failure-Resilience Testing

DIE reserves the right to conduct reliability and failure-resilience tests on the personalization facility on a periodic basis, at intervals of not less than 30 days. [Ref: Scope B B.8.14]

3.10 On-Site Engineering Staffing and On-Call Coverage (Scope B - Personalization)

The Contractor shall keep a qualified personalization/technical engineer physically present at the personalization facility throughout DIE's normal business/operating hours (8:00 a.m. to 6:00 p.m., Monday to Friday, excluding public holidays) to support routine operations, equipment upkeep, and the turnaround and throughput targets set out in Sections 3.1 and 3.2.

- **On-Call Responsibility Outside Business Hours:** It shall be the Contractor's sole responsibility, at its own cost, to maintain a documented on-call roster of suitably qualified technical experts available outside normal business hours - including during any Extended Operating Shift under Section 3.1 - so that the Contractor continues to meet all turnaround-time, throughput and other SLA obligations under this Agreement regardless of the hour at which support is required.
- **Roster & Escalation Contacts:** The Contractor shall furnish DIE, prior to commissioning and whenever updated, with the current on-site duty roster and an out-of-hours escalation contact list (names, roles, and direct contact numbers) for the on-call engineers, so that DIE can raise an urgent issue at any hour.

Deduction / Surcharge Type	Applicable Base Rate & Formula	Key Billing Conditions & Caps
Throughput Delay (Priority Levels 1 & 2)	First 2 hours of delay: 0.25% per passport. Beyond 2 hours: 0.1% per hour (or part thereof) per passport.	Calculated per affected passport. Applied to the daily personalization payment.
Throughput Delay (Priority Level 3)	First 24 hours of delay: 1.0% per passport. Beyond 48 hours: 0.5% per calendar day (or part thereof) per passport.	Calculated per affected passport. Applied to the daily personalization payment.
Volume Shortfall Penalty (Missed shift targets)	Formula-based deduction: $\text{Penalty \%} = 100 * (\text{P_total} - \text{P_completed}) / \text{P_total}$	P_total is the lower of valid requests submitted or shift expected volume. P_completed is the volume returned within shift. Overridden if throughput penalty is higher (non-cumulative).
Surcharge for Spoiled Booklets (Contractor Error)	USD \$50.00 equivalent in LKR per booklet spoiled or damaged due to technical/operational error.	No upper limit per billing cycle. If the surcharge exceeds 60% of the invoice amount (after penalties), the balance is carried forward to the next month.
Daily Penalty Cap (Aggregate Deductions)	Maximum daily penalty is capped strictly at 60% of the daily personalization invoice.	The penalty percentage is rounded upward to the nearest whole percentage point. Excludes booklet surcharges.

4. Security, Compliance, and Data Protection Standards

Because passport personalization involves highly sensitive national security data and citizen biographic/biometric records, the personalization facility and the supporting software environments must comply with the highest level of logical and physical security protocols.

4.1 Physical and Environmental Controls

The Contractor shall establish, manage, and maintain the following physical controls at primary and secondary sites (where applicable):

- **CCTV Surveillance:** Installation and 24/7 maintenance of high-definition CCTV cameras covering all production, storage, entry/exit, and audit points. All video footage must be retained locally for a minimum of 180 calendar days. DIE must be provided with real-time, read-only remote access to the CCTV system.SLA
- **Electronic Access Control (EACS):** Biometric and proximity-card access controls for all restricted zones. All access attempts must be logged in a tamper-evident system database. Access logs shall be made fully transparent to DIE and retained for the duration of the contract.
- **Non-Returnable Storage policy:** In compliance with strict defense-grade data protection, any hardware components that have stored sensitive biographic/biometric data or active cryptographic keys (such as certified HSMs, central servers, workstations, storage drives, and solid-state disks) must be permanently retained by DIE upon replacement or contract termination. The Contractor is prohibited from removing any such components from DIE premises.
- **Equipment Movement Control:** Movement of any equipment into or out of the personalization facility shall be permitted only with DIE's prior approval and under the supervision of authorized DIE personnel; all such movements shall be logged and retained for audit and security review. [Ref: Scope B B.5.6]

4.2 Logical Data Protection and Permanency Purging

To ensure absolute compliance with Sri Lankan data sovereignty, national security guidelines, and international privacy laws:

- **Permanency Purging SLA:** All bearer-specific biographic and biometric data must be permanently and cryptographically purged from all temporary databases, printer memories, queue logs, and local buffers within three (3) hours of the physical document's successful handover to DIE. No citizen records shall be retained within the personalization subsystem except standard transactional audit logs (which contain only metadata, document serial number, and timestamp).
- **Regulatory Compliance:** The personalization facility and software architecture must achieve 100% compliance with Sri Lanka's Personal Data Protection Act (PDPA) No. 9 of 2022, the Electronic Transactions Act No. 19 of 2006, and the Computer Crimes Act No. 24 of 2007. Any modifications required to maintain compliance with subsequent amendments shall be executed by the Contractor immediately at no additional cost to DIE.
- **Network Isolation:** No hardware or software within the personalization facility shall be connected to any external network or internet channel. Approved software updates, security

hotfixes, or vendor patch deployments must be routed strictly through DIE's authorized secure network and executed under the active supervision of DIE ICT personnel.

- **Data, Backup & Log Retention SLA:** The Contractor shall protect the integrity, availability and controlled retention of all data, backups, audit trails and logs of the personalization system. Long-term retention arrangements shall be agreed with DIE, and DIE shall have unrestricted access to these records, including the tools required to search, retrieve, export and extract them on demand. [Ref: Scope B B.5.10]
- **Ongoing Compliance Currency:** The Contractor shall ensure the personalization system remains compliant with applicable ICAO/ISO standards and Government of Sri Lanka regulations for the duration of the contract, including periodic review, audit and upgrade where necessary, at no additional cost to DIE. [Ref: Scope B B.5.9]

PROCUREMENT DOCUMENT - PKI DIE&E