

# **Technical Requirements for the PPP project on biometric passport and ID card issuance services**

October 2024

## TABLE OF CONTENTS

ABBREVIATIONS AND DEFINITIONS .....	3
1. PROJECT DESCRIPTION, SCOPE, AND OBJECTIVES .....	5
1.1. Context of the Project .....	5
1.2. Object and scope of the Tender .....	6
2. TECHNICAL REQUIREMENTS .....	15
2.1. Applicable standards and normative documents .....	15
2.1.1. General requirements .....	15
2.1.2. Laws and regulations .....	15
2.1.3. General Standards and Normative Documents .....	17
2.1.4. Contact interface.....	17
2.1.5. Contactless Interface .....	17
2.2. Requirements for physical infrastructure .....	19
2.2.1. Requirements for enrolment facilities (service points) .....	19
2.2.2. Requirements for personalization facility .....	19
2.2.3. Requirements for technological infrastructure .....	20
2.3. Requirements for Travel and Identity documents .....	22
2.3.1. Blank documents' manufacturing .....	22
2.3.2. Specifications for ID card .....	24
2.3.3. Specifications for Passports .....	25
2.3.4. Specimen and test documents .....	29
2.3.5. Chip and OS specifications for ID Cards .....	31
2.3.6. Chip and OS specifications for Passports .....	33
2.3.7. Middleware for ID card .....	34
2.4. Requirements for the Identity and Document Management Information System .....	36
2.4.1. Non-functional requirements for IDMIS .....	36
2.4.2. Functional requirements for IDMIS.....	40
2.5. Service level agreement KPIs .....	55
2.6. Requirements for the requested services .....	64
2.6.1. Design and implementation requirements .....	64
2.6.2. End-to-end service operations' requirements .....	66
2.6.3. Hand back requirements .....	71
2.6.4. Special provisions for design, implementation, and hand back of the Biometric data and document registry (Registry).....	83
3. ANNEXES	85

## ABBREVIATIONS AND DEFINITIONS

The list of abbreviations and definitions used in the document is provided in Table 1.

**Table 1.** Abbreviations and definitions

Abbreviations and definitions	Explanation
<b>Armenia, RA, AM</b>	Republic of Armenia
<b>BAC</b>	Basic Access Control
<b>CA</b>	Certification authority
<b>Confidential data</b>	All information processed in relation to identity and travel documents that is stored in IDMIS
<b>Contracting Authority</b>	Ministry of Internal Affairs of the Republic of Armenia
<b>CRL</b>	Certificate Revocation List
<b>CSCA</b>	Country Signing Certification Authority
<b>CSR</b>	Certificate signing request
<b>CVCA</b>	Country Validation Certification Authority
<b>DC</b>	Data center
<b>DSR</b>	Disaster recovery sight
<b>DVCA</b>	Document Validation Certification Authority
<b>EAC</b>	Extended Access Control
<b>eIDAS</b>	EU regulation on electronic Identification, Authentication, and trust Services
<b>eMRTD</b>	Electronic machine-readable travel documents
<b>Enrolment facility</b>	Premises used for the citizen biometric data enrolment, issuance (delivery) of travel and identity documents to citizens as well as overall customer support
<b>eSignature</b>	Electronic Signature
<b>“EKENG” CJSC, EKENG</b>	E-Governance Infrastructure Implementation Agency
<b>GoA</b>	Government of Armenia
<b>GM</b>	General Mapping
<b>ICAO</b>	International Civil Aviation Organization
<b>ID card</b>	National Identity Card
<b>IDMIS</b>	Identity and Documents Management Information System
<b>IM</b>	Integrated Mapping
<b>IT</b>	Information Technologies
<b>M</b>	Million
<b>MS, Migration Service</b>	Migration and Citizenship Service of the Ministry of Internal Affairs of the Republic of Armenia
<b>MFA</b>	Ministry of Foreign Affairs of the Republic of Armenia
<b>MRF</b>	Machine Readable Zone
<b>NA</b>	Not applicable

<b>Abbreviations and definitions</b>	<b>Explanation</b>
<b>NFC</b>	Near field communication
<b>OS</b>	Operating system
<b>PACE</b>	Password Authenticated Connection Establishment
<b>PIN code</b>	Personal identification number code
<b>PKI</b>	Public key infrastructure
<b>PPP</b>	Public-Private Partnership
<b>Project</b>	PPP project on biometric passport and ID card issuance services
<b>Registry</b>	Biometric Data and Document Registry, a component of the IDMIS
<b>QVCA</b>	Quality Validation Certification Authority
<b>Service Provider</b>	Winner of the PPP tender on issuing new Biometric Passports and Electronic Identity Cards
<b>SLA</b>	Service-level agreement
<b>SMS</b>	Short message service
<b>Source Code</b>	The Source Code shall contain all information in human readable form necessary to enable a reasonably skilled programmer or analyst to maintain and (or) enhance the software, and without prejudice to the generality of the foregoing, that the source code and related documentation shall contain all listings of programmers' comments, data and process models, logic manuals, and flowchart. It should also include configuration, installation and operation guides (files), dependencies and testing scripts per type of software.
<b>Tender</b>	PPP tender on issuing new Biometric Passports and Electronic Identity Cards
<b>Technical Requirements</b>	Minimum service requirements described in this document, scope of the Tender
<b>UV</b>	Ultraviolet

# 1. PROJECT DESCRIPTION, SCOPE, AND OBJECTIVES

## 1.1. Context of the Project

The Government of Armenia (GoA) represented by the Ministry of Interior Affairs aims to enter a PPP agreement on issuing new Biometric Passports (Passports) and Electronic Identity Cards (ID cards) (hereinafter – Project).

Currently the travel and ID document issuance is led by the Migration Service under the Ministry of Interior (MS) in cooperation with a local vendor. Diplomatic passport and passport issuance abroad is led with the support of the Ministry of Foreign Affairs (MFA). E-Governance Infrastructure Implementation Agency (EKENG) provides ID card certificates for authentication and eSignature. The equipment and property for passport and ID card issuance is managed by the MS as well as the MFA.

There are 126 enrolment facilities for the citizen biometric data enrolment, issuance (delivery) of travel and ID documents to citizens as well as overall customer support:

- 65 enrolment facilities in the territory of Armenia
- 61 enrolment facilities in the missions abroad (embassies and consulates in different foreign countries, also a single facility in Yerevan for diplomatic passports and ID cards): current 54 enrolment facilities are operational, 7 more are to be opened in 2024 and 15 potential new ones are planned to be opened over the next 10 years.

Historical document volumes, locations and productivity information of the enrolment facilities is provided the “Annex No. 1: Data about issued document volumes, enrolment / customer service facilities operated in Armenia and in foreign missions”.

Biometric passports and ID cards have been available in the Republic of Armenia for over 10 years, however, poor citizen experience, low uptake of modern and secure identity and travel documents as well as inefficient processes and operational risks identified have triggered a need to initiate the Project.

The Service Provider is expected to bring the know-how into the end-to-end biometric passports and ID cards issuance and distribution process, aiming to address and resolve issues highlighted below.

### ***Poor citizen experience:***

1. Identity and travel document issuance especially in peak periods takes a long time (e.g., citizen may need to wait up to 4 hours in the live queue to fill in application for a travel or ID document).
2. Process of document issuance is not user friendly – applications are signed only onsite in paper format, citizens are forced to wait in long queues (especially in peak times) to apply for a document, since online appointment booking system is not in use for all citizens.
3. Enrolment facilities do not meet a modern public service standard – physical locations are of poor condition and not convenient.
4. Citizens can apply for the travel and identity document only in less than 30 % of embassies or consulates of Armenia.

### ***Low uptake of modern and secure identity and travel documents:***

5. Old type non-biometric passports are still prevailing but provide limited security and fraud prevention features that are becoming crucial in modern times.

6. Since biometric passports uptake is low, it limits further development of digital society, for example, automated border control use case cannot be activated (handling entry and exit at border controls with automated passport systems).
7. eID card uptake is higher, but still less than half of the population poses it. This on the large scales limits the adoption of secure eID system allowing to securely access digital services or perform automated identity validation operations (e.g., for voting purposes).
8. Current ID card related infrastructure and services do not meet global security standards (e.g., eIDAS/ETSI, ISO27001), thus limiting the cross-border interoperability (e.g., recognition of Armenian eSignature cross-border).

***Inefficient processes and operational risks:***

9. Current enrolment and personalization infrastructure has limited capacity – e.g., limited number of enrolment stations, inefficient paper processes, limited productivity of personalization equipment. Thus, it does not provide an opportunity to meet citizen expectations for speed and availability of travel and identity document issuance services.
10. Current enrolment and personalization infrastructure is outdated and provides significant operational / business continuity risk of using IT system and equipment that is at the end of its lifecycle or in some cases no longer supported (e.g., current eID chip (applet) and middleware).
11. Lack of long-term partnership that would ensure continuous improvement of operations, security, and adherence to modern industry standards.

The main goal of the Project is to support Armenia’s digital transformation and high-quality service delivery to the population via facilitating the establishment of long-term public – private partnership (PPP) for issuance and distribution of biometric passports and ID cards. Key objectives are focused on the following aspects:

1. Set new world class standards for the citizen experience and service quality, including reducing waiting time, lead time to issue travel and identity documents, setting new customer service standards in enrolment facilities as well as upgrading physical conditions of the facilities to the best international standards.
2. Increase uptake and usage of secure and global standards compliant travel and identity documents, enabling development of digital society in Armenia, incl. increased uptake of advances eServices and other automation opportunities (e.g., identity verification for voting, automated border crossing, etc.).
3. Replace outdated IT infrastructure to improve process security, efficiency and manage operational risks related to legacy solutions as well as adopting innovative solutions by continuously aligning it with industry best standards.

**1.2. Object and scope of the Tender**

The object of the tender is the managed end-to-end services for supplying the citizens with secured identity and travel documents.

The Contract will be signed for 11 years between the appointed body by the Ministry of Interior Affairs (Contracting Authority) and the winner of the Tender (the Service Provider).

The Service provider is expected to provide the citizens of Armenia and foreigners, where applicable, the document types provided below in the table.

**Table 2.** Types of documents and document demand estimations

No.	Type of document	Document type	<sup>1</sup> Document validity, years	Projected quantity (operational phase)
1.	Biometric Passport of the citizen of the Republic of Armenia (Regular)	ID3	10	2 222 220
2.	Biometric Passport of the citizen of the Republic of Armenia (Diplomatic)	ID3	5	5 560
3.	Service Passport of the citizen of the Republic of Armenia	ID3	5	11 110
4.	1951 Refugee Convention Travel Document	ID3	10	11 110
5.	1954 Stateless Persons Convention Travel Document	ID3	5	11 110
6.	Electronic Identification Card of the citizen of the Republic of Armenia	ID1	5	4 744 450
7.	Residence Permit Electronic Card of the Republic of Armenia	ID1	1 or 5 years	166 665
8.	Refugee's Electronic Identification Card of the Republic of Armenia	ID1	5	16 665
9.	Stateless Persons Electronic Identification Card	ID1	5	16 665
10.	Foreign Diplomats Electronic Identification Card	ID1	5	16 665
11.	Non-Residents and Foreign Citizens Electronic Identification Card of the Republic of Armenia	ID1	5	8 335
12.	Passport specimens	ID3	NA	2500
13.	ID card specimens	ID1	NA	3000
14.	Test (white cards with electronic functionalities)	ID1	NA	1000

ID1 ID card format cards shall comprise the latest achievements in identity cards technology and security. All types listed above will have the same design, the different subtypes will be identified with a specific layout at personalization stage.

The new generation ID3 travel documents booklet technology and security shall comprise the latest achievements in ICAO Doc 9303. All (passport) types listed above will have the same design, the different subtypes will be identified with a specific layout at personalization stage.

The estimated document volumes per year for the duration of contract are in the Annex No 3.

The scope of this Contract includes end-to-end managed services in relation to issuance of Passports and ID cards, incl. but not limited to:

1. Design, implementation, operations and maintenance (O&M) of the physical infrastructure.

<sup>1</sup> According to ISO/CEI 7810 standard

2. Design, implementation, and O&M of integrated Identity and Document Management Information System (IDMIS) (refer to “Picture 1. Conceptual diagram of the scope of this Tender”), incl. all hardware, software, and equipment necessary to provide citizens with travel and identity documents from booking an appointment to document delivery to citizen.
3. Design and delivery of enrolment operations (end-to-end front office customer service operations from pre-enrolment to document issuance (delivery) to citizen, incl. all the necessary resources and supporting processes).
4. Design and delivery of personalization operations (end-to-end service from personalization request to document delivery to citizen, incl. all the necessary resources supporting processes).
5. Design, production, and supply (logistics) operations of travel and identity document blanks.

A more detailed breakdown of end-to-end managed services in relation to issuance of Passports and ID cards in the scope of the Contract are in Table 3 below.

The Service Provider is expected to assume full end-to-end responsibility of operations (with specific expectation highlighted in this chapter) making sure biometric passports and ID cards are available for citizens on Armenia and foreigners, where applicable, in accordance with SLAs and the technical requirements specified in this document, even if specific process or function is not mentioned in the list below.

List of processes and functions should be completed and described in full when preparing a “Process manual and operating procedures” document described under chapter “2.6.1. Design and implementation requirements”:

**Table 3. Roles and Responsibilities of the Service provider**

Nr.	Roles and Responsibilities of the Service provider
<b>1</b>	<b>Enrolment services</b>
1.1.	End-to-end customer front office service related to travel and identity card document issuance, incl. biometric data enrolment, processing of applications, document issuance (delivery) to citizens, registration authority functions for the qualified eSignature, customer support and help desk operations related to lifecycle of the document
1.2.	Design, implementation, and O&M of customer information and self-service system, incl. appointment booking system
1.3.	Design, implementation, and O&M of payment collection system
1.4.	Design, implementation, and O&M of queuing system
1.5.	Management of document lifecycle events, incl. PIN
1.6.	Design, implementation, and O&M of PIN replacement system
1.7.	Design, implementation, and O&M of document enrolment and issuance system
1.8.	Design, construction/renovation, and O&M of enrolment facilities
1.9	Provision of adequate and reliable internet connectivity at enrolment, personalization, data center facilities and disaster recovery site (excluding foreign missions and MFA facilities) sufficient to deliver Services and Operations, and maintenance of the connectivity through the duration of the Project
1.10.	Design, construction/renovation, and O&M of server room facilities
1.11.	Design, implementation, and O&M of private cloud for enrolment services
1.12.	Compliance assurance
1.13	Consulting of Contracting Authority regarding GoA process efficiency improvement and / or new functions (e.g., vetting process efficiency improvement)
1.14	Enrolment reporting to Contracting Authority



Nr.	Roles and Responsibilities of the Service provider
<b>2</b>	<b>Personalization services</b>
2.1.	End-to-end logistical and personalization (production) operations
2.2.	Design, construction/renovation, and O&M of personalization facilities
2.3.	Design, implementation, and O&M of document personalization system
2.4.	Design, construction/renovation, and O&M of server room facilities
2.5.	Design, implementation, and O&M of private cloud for personalization services
2.6.	Design, implementation, and O&M of ICAO PKI system
2.7.	Design, implementation, and O&M of PIN system
2.8.	Compliance assurance
2.9.	Consulting of Contracting Authority regarding GoA process efficiency improvement and / or new functions (e.g., participation in ICAO organization)
2.10.	Personalization reporting to Contracting Authority
<b>3</b>	<b>Travel and identity document blank production</b>
3.1.	Prepare final biometric passport aesthetic design, considering input provided by the Contracting Authority
3.2.	Prepare final ID card aesthetic design, considering input provided by the Contracting Authority
3.3.	Production and supply of ID card blanks
3.4.	Production and supply of Passport blanks
3.5.	Design, implementation, and O&M (continuous delivery) of middleware
3.6.	Logistical operations
3.7.	Compliance assurance
3.8.	Production reporting to Contracting Authority

Below are the roles and responsibilities as well functions that are expected to be retained within the Contracting Authority:

**Table 4.** Roles and Responsibilities of the Contracting Authority

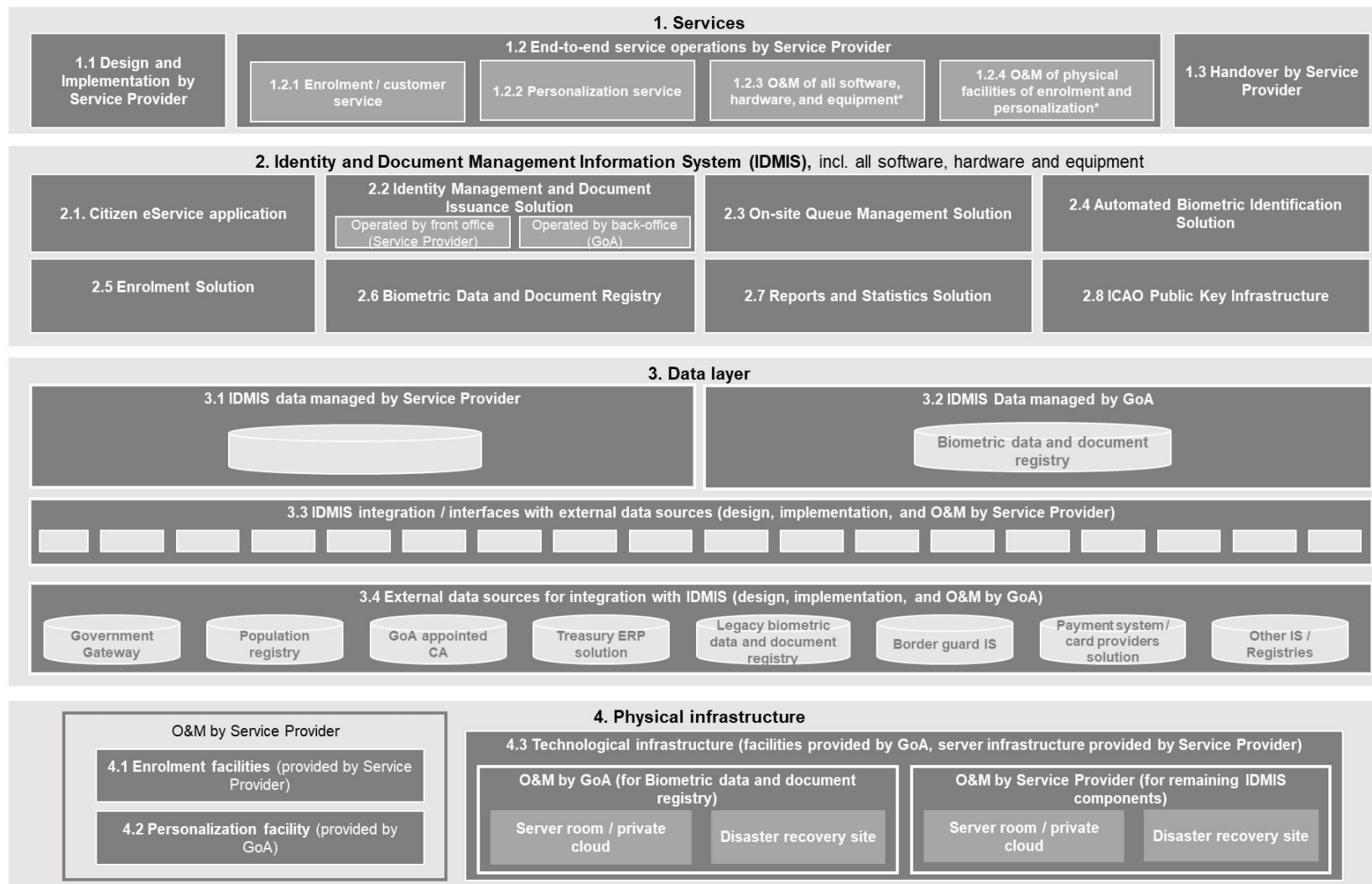
Nr.	Roles and Responsibilities of the Contracting Authority
1	Design, development and implementation, M&O of integration interfaces with Government managed information systems or registers necessary for the service of passport and ID cards
2	Design, development and implementation, M&O of Population register and its integration interface necessary for the service of passport and ID cards
3	M&O of historic (legacy) Biometric data and document registry and its integration interface necessary for the service of passport and ID cards and / or data preparation for migration.  Note: Service provider may choose if to realize integration interface between IDMIS and legacy Biometric data and document registry or to migrate data from legacy registry to new Biometric data and document registry.
4	M&O of new Biometric data and document registry (one of the components of IDMIS) and its integration interface necessary for the service of passport and ID cards (however,

Nr.	Roles and Responsibilities of the Contracting Authority
	<p>Service provider will provide maintenance services of relevant IT infrastructure as per specific requests by the GoA during the Contract duration).</p> <p>Note: Biometric data and document registry (one of the components of IDMIS) shall be handed over to the Contracting Authority (differently than other IDMIS components) right after the implementation.</p>
5	<p>Provisioning and supervision of personalization facilities, incl. but not limited to right to enter, right to audit and access any data or information related to activities undertaken in the facilities (however, Service Provider will assume responsibility to update and maintain conditions of the facilities according to the Technical Requirements)</p>
6	<p>Provisioning and supervision of data center facilities for passport and ID card related services (however, Service Provider will assume responsibility to update and maintain conditions of the facilities according to the Technical Requirements).</p> <p>Note: All IDMIS components will need to be installed in the data center location provided by the GoA, but operation of this data center shall be managed by the Service Provider (except for the data bases of the Biometric data and document registry).</p> <p>Regardless of the data center location or who assumes the responsibility of operations; all the necessary software and hardware shall be provided by the Service Provider.</p>
7	<p>Provisioning and supervision of disaster recovery facilities for passport and ID card related services (however, Service provider will assume responsibility to update and maintain conditions of the facilities according to the Technical Requirements).</p>
8	<p>GoA remains responsible for the sunset of the GoA facilities that will no longer be used for passport and ID card related services (terminations of the lease (if relevant), post directions to new facilities at the door, etc.).</p>
9	<p>Provisioning and compliance control of ID card certificates for the authentication and eSignature; incl. selection, management, and control of its provider (CA will be appointed by the GoA)</p>
10	<p>Operations of the following enrolment back-office functions (via access rights in the IDMIS system) by the Service Provider):</p>
10.1	<p>Granting travel and identity document (authorization of the application), after front office employees submit the verified and eligible applications for travel and identity documents</p>
10.2	<p>Biometric verification and / or adjudications, in cases when the identity of applicant cannot be reliably verified by the data available to the front office employee</p>
10.3	<p>Access rights management of all GoA users (however, Identity and Access Management IT solution design, development and implementation, M&amp;O to be provided by Service Provider)</p>
11	<p>Dispute resolution, should the Service provider be not able to solve customer complaints as a first point of contact</p>
12	<p>Transport of personalized documents to foreign missions</p>
13	<p>Operations of enrolment services in foreign missions and MFA facilities in Yerevan, incl. operations of necessary hardware and software, physical and network infrastructure installed in the premises of MFA, incl. all improvement, reconstruction works or maintenance of premises (however, Service provider will provide maintenance of IT infrastructure as per specific requests by the MFA and agreed SLAs)</p>
14	<p>Participation in Public Key Directory (organizational role)</p>

Nr.	Roles and Responsibilities of the Contracting Authority
15	Storage of ICAO keys for biometric passports issued prior the Contract, share keys with ICAO public directory.
16	Provide input on biometric passport aesthetic design, work together with Service Provider to align final aesthetic design
17	Provide input on ID card aesthetic design, work together with Service Provider to align final aesthetic design
18	The GoA will classify the personalization site as “special importance facility” and will ensure external guarding by the Armenian police for 24 hours a day
19	The GoA will ensure external guarding of enrolment facilities by the Armenian police for 24 hours a day
20	Compliance control, including access and right to audit information system user rights, security controls and logs data
21	Cooperate with the Service Provider, transfer knowledge of current operations, act as a counterpart when aligning planning and design documents

**Important note:** roles and responsibilities split shall follow Information System Management Board Meeting Minutes No. 05/2022, dated December 27, 2022 (Annex No. 4: Minimum Security Principles). In case if any conflict with the description of the services in this tender, the protocol decision shall prevail.

Conceptual diagram below provides a summarized overview of the scope of this Tender.



\* Except for the Biometric Data and Document Registry

**Picture 1.** Conceptual diagram of the scope of this Tender

Following chapter “2. Technical requirements”, provides the minimum service requirements in the scope of this Tender. Table below summarizes the structure of the following chapter:

No.	Chapter	Scope of the chapter
<b>2.1</b>	<b>Applicable standards and normative documents</b>	Provides a list of mandatory standards and normative acts that Service Provider must follow and adhere.
<b>2.2</b>	<b>Requirements for physical infrastructure</b>	Provides requirements for physical infrastructure that Service provider is responsible to design, implement and provide O&M services.
2.2.1	Requirements for enrolment facilities	
2.2.2	Requirements for personalization facility	
2.2.3	Requirements for technological infrastructure	
<b>2.3</b>	<b>Requirements for travel and identity documents</b>	Provides requirements for travel and identity documents that Service Provider must implement and adhere in the scope of this Tender.
2.3.1	Blank documents’ manufacturing	
2.3.2	Specifications for ID card	
2.3.3	Specifications for Passports	
2.3.4	Specimen and test documents	
2.3.5	Chip and OS specifications for ID cards	
2.3.6	Chip and OS specifications for Passports	
2.3.7	Middleware for Identity Card	
<b>2.4.</b>	<b>Requirements for the Identity and Document Management Information System (IDMIS)</b>	Provides functional and non-functional requirements for Identity and Document Management Information System (IDMIS) and its functional areas, that Service Provider must design, implement, and provide O&M services.
2.4.1	Non-functional requirements for IDMIS	
2.4.2	Functional requirements for IDMIS	
<b>2.5</b>	<b>Service level agreement KPIs</b>	Provides a list of Service level agreement KPIs and its values that Service Provider will need to adhere in the scope of this Tender.
<b>2.6</b>	<b>Requirements for requested services</b>	

No.	Chapter	Scope of the chapter
2.6.1	Design and implementation requirements	Provides requirements for design and implementation phase of the project (incl. timelines, documentation, etc.)
2.6.2	End-to-end service operations' requirements	Provides requirements for operations' during the operational phase of the Tender.
2.6.3	Hand back requirements	Provides requirements for the hand back phase of the project (incl. timelines, documentation, licensing, warranty services, etc.)
2.6.4	Special provisions for design, implementation, and hand back of the Biometric data and document registry	Provides specific provisions / requirements for design, implementation and hand back services for Biometric data and document registry since this solution will be handed over to GoA immediately after successful implementation. Therefore, more output time results need to be specified.

## **2. TECHNICAL REQUIREMENTS**

### **2.1. Applicable standards and normative documents**

#### **2.1.1. General requirements**

- If multiple standards set requirements for the same aspect, the standard with higher or stronger requirements has precedence.
- If multiple standards set incompatible requirements for the same aspect, the Contracting Authority is eligible to choose the standard to follow at its full discretion.
- Upon difference between the requirements specified in contractual documents and the requirements proceeding from the following legislative acts and regulation of technical descriptions issued on their basis, the requirements proceeding from legislative acts shall prevail but the contractual documents' terms shall be preserved to the maximum amount possible.
- All those standards are applicable to be comply with and for the one requested, to be provide evidence of compliance.
- All the requirements detailed in the proposal are required, unless it is specifically marked that the requirement is optional. Optional requirements will be evaluated and will count towards the evaluation score, but are not mandated to be implemented, if not indicated in the proposal of the Service provider.

#### **2.1.2. Laws and regulations**

- Civil Code. URL: <https://www.arlis.am/DocumentView.aspx?DocID=165457>
- Law on Diplomatic Service
- Minister of Foreign Affairs Order 2/757-N from 29 December 2010
- Minister of Foreign Affairs Order 2/1683-N from 30 December 2008
- Law on public and private notice over the internet. URL: <https://www.arlis.am/documentview.aspx?docID=87385>
- Law on electronic document and electronic digital signature. URL: <https://www.arlis.am/DocumentView.aspx?DocID=120911>
- Law on Identification cards. URL: <https://www.arlis.am/DocumentView.aspx?DocID=158650>
- Law on personal data protection. URL: <https://www.arlis.am/DocumentView.aspx?DocID=132745>
- Law on passport of the citizen of the Republic of Armenia. URL: <https://www.arlis.am/DocumentView.aspx?DocID=164946>
- Law of the Republic of Armenia on "Citizenship of the Republic of Armenia". URL: <https://www.arlis.am/DocumentView.aspx?DocID=166137>
- Law of the Republic of Armenia "On Foreigners". URL: <https://www.arlis.am/DocumentView.aspx?DocID=166247>
- Law of the Republic of Armenia "On the State Register of Population". URL: <https://www.arlis.am/DocumentView.aspx?DocID=120904>
- Law of the Republic of Armenia "About registration plate of public services". URL: <https://www.arlis.am/DocumentView.aspx?DocID=144992>
- Government Decision 28.04.2022, 585-N On determining permissible limits of contractual and direct obligations of public-private partnership. URL: <https://www.arlis.am/DocumentView.aspx?docID=162421>
- Government Decision 31.08.2015, 1093-N On defining the security, interoperability and general technical requirements of electronic systems used by state and local self-government bodies for the provision of electronic services or performance of operations. URL: <https://www.arlis.am/DocumentView.aspx?DocID=152169>

- Government Decision 19.12.2019, 1849-N On procedure for exchange of personal data through the electronic information system to confirm and the existence of the Republic of Armenia n 192 of February 16, 2017 decision regarding validity. URL: <https://www.arlis.am/DocumentView.aspx?DocID=137681>
- Government Decision 04.08.2005, 1596-N, On approval of the procedure for accreditation of electronic digital signature certification centers. URL: <https://www.arlis.am/DocumentView.aspx?DocID=47158>
- Government decision 25.05.2017, 572-N, on establishing the procedure for the use of electronic documents and electronic digital signatures in state bodies, on establishing the general technical requirements for the electronic systems used when purchasing the services or actions provided by state and local self-government bodies in electronic form using electronic digital signatures, and repealing Decree No. 1595 of 2005 of the Government of the Republic of Armenia. URL: <https://www.arlis.am/DocumentView.aspx?DocID=161330>
- Government decision 20.02.2014, 217-A About recognizing the authorized body and operator. URL: <https://e-gov.am/gov-decrees/item/24021/>
- Government decision 27.03.2014 375-N On the procedure for the organization and financing of the beneficiaries of the social package, as well as the employees of the organizations providing primary health care and narrow professional services guaranteed by the state with free and preferential conditions, the medical care and service guaranteed by the state with free and preferential conditions, their free and preferential medical care guaranteed by the state and the package of service services, the procedure for the creation and management of electronic databases for the purpose of access to the package, as well as on the approval of the model form of the contract to be concluded between the Ministry of Health of the Republic of Armenia and the companies providing insurance services. URL: <https://www.arlis.am/DocumentView.aspx?DocID=157369>
- Government decision 04.08.2005 1594-N On the approval of the authorized body of the government of the Republic of Armenia performing the accreditation of electronic digital signature verification centers. URL: <https://www.arlis.am/DocumentView.aspx?DocID=136335>
- Government decision 04.08.2005 1596 N On approval of the procedure for accreditation of electronic digital signature certification centers. URL: <https://www.arlis.am/DocumentView.aspx?DocID=47158>
- Government decision 04.08.2005, 1597N On approval of the procedure for maintaining the book (register) of accredited certification centers of electronic digital signature. URL: <https://www.arlis.am/DocumentView.aspx?DocID=47159>
- Government decision 25.01.2008 116-N On approval of the technical criteria for the services provided by the electronic digital signature certification centers for accreditation. URL: <https://www.arlis.am/DocumentView.aspx?DocID=42747>
- Government decision 01.03.2018, 285 N On establishing the procedure for issuing and providing electronic digital signature certificates inserted in other types of material media, in addition to the issuance of electronic digital signature certificates inserted in the identification card. URL: <https://www.arlis.am/DocumentView.aspx?DocID=120696>
- Government decision No 175-N dated 09.02.2023 On the selection, development, evaluation and prioritization of public investment programs. URL: <https://www.arlis.am/DocumentView.aspx?docID=174111>
- Law HO-113-N On Public-Private Partnership. URL: <https://www.arlis.am/DocumentView.aspx?DocID=154385>
- Government decision No 1183-N dated 28.07.2022 on the PPP procedure, the database establishing the procedure for the creation and management of a database on public-private partnership programs, the areas of public services provided within the framework of public-private partnership programs, the subdivision of public-private partnership, the form and submission period of the report on the implementation of the public-private partnership program and on repealing the Decision of GoA No. 1241-N dated September 20, 2012". URL: <https://www.arlis.am/DocumentView.aspx?docID=166779>
- Information System Management Board Protocol No. 05/2022, dated December 27, 2022



### **2.1.3. General Standards and Normative Documents**

- GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- ITU-R Recommendation BT.601 /BT.709;
- Payment Card Industry (PCI) Card Production and Provisioning (CPP) – Physical Security Requirements, v2.0 – December 2016 (compliance requested)
- Payment Card Industry (PCI) Card Production and Provisioning (CPP) – Logical Security Requirements, v2.0 – December 2016 (compliance requested);
- ISO/IEC 2859-1:1999 Sampling procedures for inspection by attributes — Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection;
- ISO/IEC 7810: Identification Cards – Physical Characteristics;
- ETSI TS 119 461 V1.1.1 (to the extent relevant for trust service enrolment and lifecycle services)
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, and its successive legal acts URL: [http://eurlex.europa.eu/legal-content/ET/TXT/?uri=OJ%3AJOL\\_2014\\_257\\_R\\_0002](http://eurlex.europa.eu/legal-content/ET/TXT/?uri=OJ%3AJOL_2014_257_R_0002)
- RFC6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP URL: <https://tools.ietf.org/html/rfc6960>
- RFC 2119. Key words for use in RFCs to Indicate Requirement Levels. URL: <https://tools.ietf.org/html/rfc2119>
- RFC 3280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
- Profile. URL: <https://www.ietf.org/rfc/rfc3280.txt>
- RFC 4511. Lightweight Directory Access

### **2.1.4. Contact interface**

- ISO/IEC 7816-1: Identification cards - Integrated circuit(s) cards with contacts. Part 1: Physical Characteristics,
- ISO/IEC 7816-2: Identification cards - Integrated circuit(s) cards with contacts. Part 1: Cards with contacts - Dimensions and location of the contacts,
- ISO/IEC 7816-3: Identification cards - Integrated circuit(s) cards with contacts. Part 3: Electronic, signals and transmission protocols,
- ISO/IEC 7816-4, Identification cards - Integrated circuit(s) cards with contacts. Part 4: Organization, security, and commands for interchange,
- ISO/IEC 7816-5: Identification cards - Integrated circuit(s) cards with contacts. Part 5: Registration procedure for application identifiers,
- ISO/IEC 10373: "Identification Cards - Test Methods"

### **2.1.5. Contactless Interface**

- ISO/IEC 14443-1 Identification cards - Contactless integrated circuit(s) cards - Proximity cards Part 1: Physical Characteristics;
- ISO/IEC 14443-2 Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface;
- ISO/IEC 14443-3 Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anti-collision;

- ISO/IEC 14443-4 Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol;
- ISO/IEC 15408-1: Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model;
- ISO/IEC 15408-2: Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements JTC1/SC27;
- ISO/IEC 15408-3: Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements;
- ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements;
- ISO/IEC CD 24789-2: Identification cards -- Card service life -- Part 2: Methods of evaluation;
- Common Criteria for Information Technology Security Evaluation version 3.1 Revision 4, September 2012, <https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R4.pdf>
- ICAO Doc 9303 "Machine Readable Travel Documents" (Seventh Edition — 2015);
- ICAO TAG MRTD/NTWG Technical Report "Biometrics Deployment of Machine-Readable Travel Documents" Version 2.0;
- ICAO TAG MRTD/NTWG Technical Report "PKI for Machine Readable Travel Documents Offering ICC Read-Only Access" Version 1.1;
- ICAO TAG MRTD/NTWG Technical Report "Use of Contactless Integrated Circuits in Machine Readable Travel Documents" Version 4.0;
- ICAO TAG MRTD/NTWG Technical Report "RF Protocol and Application Test Standard for Epassport - Part 3" version 2.06, March 10, 2014;
- ICAO TAG MRTD/NTWG Technical Report "Travel Document Deviation List issuance" Version 1.11, May 21, 2014;
- Supplement to ICAO Doc 9303 — Release 14, May 13, 2014;
- ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents Part 1: Best Practices" Version 3.4, January 2010;
- "Advanced Security Mechanisms for Machine Readable Travel Documents", BSI TR-03110, Part 1 and 3, Version 2.10 of 20 March 2012.

## 2.2. Requirements for physical infrastructure

### 2.2.1. Requirements for enrolment facilities (service points)

Reference	Description of Technical requirements
Req. 1.	<p>The number of enrolment facilities operated in the territory of Armenia will be defined by the Service Provider, considering the following requirements:</p> <ul style="list-style-type: none"> <li>• At least twelve (12) enrolment facilities shall be deployed, operated and maintained in geographic / administrative centers of the Republic of Armenia (at least 12 service points).</li> <li>• A single (1) or up to three (3) centralized facilities shall be established in Yerevan (number of facilities operated in Yerevan cannot exceed three (3)).</li> </ul> <p>Currently operated enrolment facilities are provided in the Annex No 1 “Data about issued document volumes, enrolment / customer service facilities operated in Armenia and in foreign missions”. Service Providers will be invited to visit the sites during the tender process.</p>
Req. 2.	<p>Each enrolment facility in Armenia that will be operated by the Service provider shall be refurbished during the implementation phase and maintained during the contract period according to the requirements set in the Annex No 2 “Requirements for enrolment facilities characteristics”.</p>
Req. 3.	<p>All equipment and furniture required to bring the facilities up to the required standards is to be supplied by the Service Provider.</p>
Req. 4.	<p>Enrolment facilities will act as Registration Authorities for a qualified eSignature. Compliance to applicable eIDAS regulations and ETSI TS 119 461 V1.1.1 standard is requested and shall be proven by annual audits from an external accredited company.</p>
Req. 5.	<p>As part of the design, each enrolment facility must deploy physical detectors to set off an alarm when an unauthorized or unusual activity or hazard within the physical premises is detected.</p>
Req. 6.	<p>Each enrolment facility shall be guarded by Police free of charge for Service provider (cost assumed by GoA).</p>

### 2.2.2. Requirements for personalization facility

Reference	Description of Technical requirements
Req. 7.	<p>ID card and Passport personalization will be carried out in the central personalization facility in Yerevan in the premises provided by the GoA. Service Providers will be invited to visit the site during the tender process.</p> <p>The building will be provided by GoA with:</p> <ul style="list-style-type: none"> <li>• Sufficient space for the installation of equipment and performance of operations</li> <li>• Electric wiring - armor doors</li> <li>• Window bars</li> <li>• Continuous illumination</li> </ul>

Reference	Description of Technical requirements
	<ul style="list-style-type: none"> <li>Alarm system connected to the closest police station.</li> </ul>
Req. 8.	The design, renovation and O&M of this personalization facility will be a responsibility of the Service Provider.
Req. 9.	The Service Provider shall provide the factory infrastructure for the personalization of identity and travel documents under the international standards required in this document and its annexes, such as the recommendations of the ICAO Doc. 9303, seventh edition, which guarantee high levels of availability, performance and security in operation for the management of inputs and the graphic and electronic personalization of the documents requested.
Req. 10.	Compliance to PCI CPP standard is requested and proven by annual audits from an external accredited company.
Req. 11.	Compliance to ISO 27001 standard is requested and proven by annual audits from an external accredited company.
Req. 12.	<p>In the design phase of the project, Service Provider shall propose a design concept of personalization facility layout and key principles of security measures to be applied (e.g., access to authorized personnel throughout the facility is logged through automated means for each individual with unescorted physical access into each environments of the facility with information to identify the individual and date of time of entry; the need for an airgap network for separating the personalization environments from internet connectivity is a fundamental requirement to prevent cybersecurity attacks against critical and sensitive assets).</p> <p>The proposed design concept shall be aligned with the GoA.</p>

### 2.2.3. Requirements for technological infrastructure

Reference	Description of Technical requirements
Req. 13.	<p>Service provider must provide, design and implement all the hardware infrastructure necessary for successful operations that meet high availability requirements (applicable for all IT solution and use cases in the scope of this tender):</p> <ul style="list-style-type: none"> <li>Main data center to be operated by the Service provider (for IDMIS operations);</li> <li>Disaster recovery site (DRS) to be operated by the Service provider (for IDMIS operations);</li> <li>Data center to be operated by the Contracting Authority (for operations Biometric data and document registry and storage of the backup copy of the operational data stored in the IDMIS databases).</li> </ul> <p>Final technological architecture will need to be designed and aligned with Contracting authority in the design phase of the project.</p>
Req. 14.	<p>The Service provider must design and implemented three fully independent environments:</p> <ul style="list-style-type: none"> <li>PROD - production environment;</li> <li>DEV - development environment;</li> </ul>

Reference	Description of Technical requirements
	<ul style="list-style-type: none"> <li>• TEST - a test environment is an environment, where a new (or updated) functionality is loaded for testing.</li> </ul>
Req. 15.	Infrastructure that is necessary for the operations for Biometric data and document registry and storage of the backup copy of the operational data stored in the IDMIS databases will need to be placed in the data center provided by the GoA. GoA will assume the responsibility for the operations of the selected data center and Biometric data registry.
Req. 16.	Infrastructure that is necessary for the operations IDMIS will need to be placed in the data center and disaster recover site both provided by the Contacting Authority. Service provider will assume the responsibility for the operations of the all the IT infrastructure (except for Biometric data and document registry).
Req. 17.	<p>Service Providers will be invited to visit the premises for the data center and DRS during the tender process.</p> <p>Both premises will be provided by GoA with:</p> <ul style="list-style-type: none"> <li>• Sufficient space for the installation of equipment and performance of operations</li> <li>• Electric wiring - armored doors</li> <li>• Window bars</li> <li>• Continuous illumination</li> <li>• Alarm system connected to the closest police station.</li> </ul>
Req. 18.	The Service provider must ensure the high availability and disaster recovery solution to meet the SLA as per chapter “2.5 Service level agreement KPIs”.
Req. 19.	<p>The IT solutions in scope of this tender will be redundant in active-passive mode in a Disaster Recovery Site (DRS) according to a backup plan validated with the Contracting Authority during the Setup phase of the project, in order to guarantee continuity of operation.</p> <p>DRS shall be ready to be used and secured at go live.</p>
Req. 20.	<p>When passive, the DRS will be able to manage:</p> <ul style="list-style-type: none"> <li>• The full dataflow of the IDMIS with data replicated in real time,</li> <li>• When active, the DRS will be able to manage: <ul style="list-style-type: none"> <li>○ 100 % of daily Passport’s volumes in 1 day;</li> <li>○ 50% daily ID cards volume in 1 day.</li> </ul> </li> </ul>
Req. 21.	The Service provider must ensure the possibility and assistance to transfer IDMIS to another data center without performing significant development works of system components.
Req. 22.	<p>The Biometric database shall be sized to host all the necessary biographic data:</p> <ul style="list-style-type: none"> <li>• 20 million records for the fingerprints,</li> <li>• 10 million records for the portraits.</li> </ul>
Req. 23.	Compliance to ISO 27001 standard is requested and proven by annual audits from an external accredited company.

## 2.3. Requirements for Travel and Identity documents

### 2.3.1. Blank documents' manufacturing

Reference	Description of Technical requirements
Req. 24.	The Service Provider shall cooperate with the Contracting Authority and shall be obliged to follow its instructions for the development of the design of the security features for all Identity and travel documents. In addition to that, Service Provider is expected to actively participate in the GoA working group capable of monitoring technological developments and safety and proactively provide suggestions for improvement of the security features of Identity and travel documents.
Req. 25.	The Service Provider shall ensure that selected Document blank / blank manufacturing provider is certified as per ISO 14298 "Security management system for secure printing" by Intergraf and listed in the following list of certified organizations: <a href="https://intergrafconference.com/index.php/list-of-certified-companies">https://intergrafconference.com/index.php/list-of-certified-companies</a> .
Req. 26.	The Service Provider shall be certified according to ISO 9001 and ISO27001 standards for information security management in their latest versions for the duration of the Contract.
Req. 27.	Contracting Authority shall have a right to visit the blank manufacturing factory and order independent audit to test compliance to the following standards: ISO 14298, ISO 9001 and ISO27001.
Req. 28.	Document blank / blank manufacturing provider cannot be changed without a written consent of the Contracting Authority.
Req. 29.	Attention shall be paid so that the facilities involved in the printing of Identity documents are appropriately secured and that the staff employed therein avail the appropriate security clearance. Appropriate security shall also be ensured during transportation of the blank documents between the facilities, as well as between the facility and the end user.
Req. 30.	Appropriate measures shall be taken to ensure that blank document production can continue in the event of catastrophic events such as fire, flooding, and equipment failure. This is achieved through the following: <ul style="list-style-type: none"> <li>• Using distributed production and issuing facilities</li> <li>• Backup production facilities</li> <li>• Emergency issuance facilities</li> <li>• Quick access to spare parts and support</li> <li>• Dual sourcing of key raw materials (such as modules, paper, ...)</li> </ul> There shall be consideration of possible failure modes in the design of the production and of the security installations in order to eliminate common faults and single points of failure.
Req. 31.	Security policies and procedures applied in the manufacturing factory must be made available for the Contracting Authority upon request.
Req. 32.	<b>Physical access and access control</b>

Reference	Description of Technical requirements
	<p>The access control shall be separated into zones and the authorization for access to each zone shall be consistent with the value of the protected elements and the requirements of the different normative constrains related to the production of blank Identity documents.</p> <p>The Supplier shall avail at his production facilities:</p> <ul style="list-style-type: none"> <li>• Wire cages or solid walls to separate the production areas</li> <li>• Armored storage rooms for ready-made, blank documents and key security features material used in production process</li> <li>• Access control between zones using security cards &amp; biometric authentication</li> <li>• Video surveillance inside and outside the production areas</li> <li>• Perimeter security control</li> <li>• Full time security personnel</li> <li>• Security Control room</li> </ul> <p>In addition, the Service Provider shall meet the requirements of Standard EN 50518 (any deviation from this standard shall be based on risk assessment).</p>
Req. 33.	<p><b>Production Materials and Accounting thereof</b></p> <p>It shall be ensured that all materials used in the production of blank documents are recorded and that the production of blank documents is matched to the orders in a manner so as to document that no blank documents or part thereof is missing.</p> <p>Any defective materials, full document and parts shall be securely destroyed and recorded.</p>
Req. 34.	<p>Periodic factory stock management report shall be provided to the Contracting Authority.</p>
Req. 35.	<p><b>Transport of blank documents</b></p> <p>The transport of blank documents and their parts shall be done under secured transport.</p>
Req. 36.	<p><b>Employees</b></p> <p>All employees must receive a security clearance through a relevant process as per company policy, which shall verify their identity and suitability for work in a high value &amp; secured production environment.</p> <p>Employees shall be accredited and monitored with the access control system allowing identify verification and access to secure areas where required based on the duties assigned.</p>
Req. 37.	<p><b>Cyber security</b></p> <p>Measures shall be taken to address various types of cyberattacks against production facilities, such as:</p> <ul style="list-style-type: none"> <li>• Viruses and other malware, compatible with the computer installations and production machines.</li> <li>• DDOS attacks through on-line application channels and online services exposed by production and issuance systems</li> </ul>

### 2.3.2. Specifications for ID card


Reference	Description of Technical requirements
	<b>General</b>
Req. 38.	The Identity card shall comply with ISO 7816 standard in a format ID1, and the substrate will be with different layers of "polycarbonate" material 100% polycarbonate.
Req. 39.	The identity card shall integrate a dual contact and contactless chip in 100% polycarbonate. The identity card shall be compliant with ISO/IEC 14443-1,-2,-3 and ISO/IEC 14443-4 A or B and compliance shall be established by an external laboratory (compliance tests to be performed before the start of operational phase).
Req. 40.	The personalized card shall have a lifespan of 5 years under normal conditions of use. The Service Provider shall provide a test report confirming the durability of the ID card based on the final design, in compliance with ISO 10373-1 and ISO 24789 using 3-D profile established by an external laboratory (compliance tests to be performed before the start of operational phase).
Req. 41.	The colors and themes of the design will be chosen in agreement with the Authorities. The Service Provider will present its methodology for design and collaboration with the Service Provider.
Req. 42.	All relevant components of ID card such as QSQR shall be eIDAS certified for the duration of the Contract. (No 910/2014 of the European Parliament and of the Council of 23 July 2014)
Req. 43.	The eID card shall comply with the requirements of the European regulation 2019/1157 article 3.
	<b>Identity Card Security Features</b>
Req. 44.	<p>The Identity card shall have a complex design comprising:</p> <ul style="list-style-type: none"> <li>• Two (2) visible color gradients (2 "rainbow"),</li> <li>• Two (2) color gradients visible under UV light (2 UV "rainbow") guilloches,</li> <li>• Fine lines,</li> <li>• Anti-scan,</li> <li>• Micro texts in positive and negative, less than or equal to 250 µm including deliberate errors,</li> <li>• OVI (Optical Variable Ink) Printing,</li> <li>• OVD (front of the card), the design of this OVD will be specific to Armenia. Changeable or multiple laser image (MLI/CLI), it will be laser engraved with the coat of arms of the country and the document number,</li> <li>• Infra-red reactive ink (drop-out or anti-stoke).</li> </ul> <p>First version of security concept for ID card design allowing to balance the proposed security feature in order to reach the maximum level of security will be aligned during the design phase, based on the security concept provided by the Service Provider during the bidding stage.</p>
Req. 45.	The card shall have tactile elements, some of which include micro-texts.
Req. 46.	The main photo shall be a color photo.




Reference	Description of Technical requirements
Req. 47.	An MRZ (machine readable zone) shall be engraved on the back of the card according to ICAO standards.
Req. 48.	The identity card shall have a barcode engraved on the back during personalization. The barcode shall contain biographic data, such as name, surname, date of birth, and other agreed elements. The exact type and the data to be included will be agreed with the Contracting Authority during the setup phase of the project.
Req. 49.	The Service Provider shall have its own design team and shall propose aesthetic design of the new ID card (initial draft to be included in his technical offer) and align it with the Contracting Authority, considering input provided by the Contracting Authority.

### 2.3.3. Specifications for Passports

Reference	Required / Optional	Description of Technical requirements
		<b>General</b>
Req. 50.	Required	The passport shall comply with the 9303 standards of the International Civil Aviation Organization (ICAO) 8 <sup>th</sup> edition.
Req. 51.	Required	The booklet is of the standard ICAO dimensions: 88 ± 0.75 mm x 125 ± 75 mm, die-cut with rounded corners.
Req. 52.	Required	The passport booklet contains: <ul style="list-style-type: none"> <li>- 40 visa pages numbered 3 to 42;</li> <li>- Polycarbonate data page that will be page 1 and 2;</li> <li>- Cover pages.</li> </ul>
Req. 53.	Required	The polycarbonate data page (pages 1 and 2) is located immediately after the cover of the booklet.
Req. 54.	Required	The personalized passport shall have a lifespan of at least ten 10 years under normal conditions of use. The Service Provider shall provide a test report confirming the durability of the booklet based on the final design, established by an external laboratory and in conformity with ISO 18745-1 (compliance tests to be performed before the start of operational phase).
Req. 55.	Required	The colors and themes of the design will be chosen in agreement with the Authorities. The Service Provider will present its methodology for design and collaboration with the Service Provider.
Req. 56.	Required	The Service Provider shall have its own design team and shall propose aesthetic design of the new Passport (initial draft to be included in his technical offer) and align it with the Contracting Authority, considering input provided by the Contracting Authority.

Reference	Required / Optional	Description of Technical requirements
Req. 57.	Required	First version of security concept for passport design allowing to balance the proposed security feature in order to reach the maximum level of security will be aligned during the design phase, based on the security concept provided by the Service Provider during the bidding stage.
		<b>The cover</b>
Req. 58.	Required	The outer surface of the cover shall be treated to resist chemicals as well as high temperatures such as when applying gilding to the cover (Coat of Arms of Armenia).
Req. 59.	Required	The passport covers shall be of the following colors: <ul style="list-style-type: none"> <li>• Ordinary = blue.</li> <li>• Diplomatic = black.</li> <li>• Service = deep red.</li> </ul>
Req. 60.	Required	The cover page of the booklet will be hot-stamped with the national emblem and the symbol reserved for electronic passports. 
Req. 61.	Required	The cover of the booklet shall incorporate fluorescent patterns under UV (365 nm). It shall comply with the BWS (Blue Wool Scale) Level 6 standard. The Service Provider shall provide the appropriate test report.
Req. 62.	Optional	The fluorescent patterns in the booklet must be perfectly aligned with the gilded elements.
		<b>Internal surface of the cover</b>
Req. 63.	Required	The inside page of the cover shall be 140g / m <sup>2</sup> security paper, +/- 5% g / m <sup>2</sup> , made from a combination of at least 20% cotton and UV dull.
Req. 64.	Required	The inside page shall incorporate a complex design, numismatic and iridescent background, consisting in particular of color rainbow (2 colors), guilloches and fine lines, micro text in positive and negative less than or equal to 250 µm and including deliberate errors.
Req. 65.	Required	The inside page shall incorporate a design printed with fluorescent ink visible under UV. These UV ink patterns shall use the symbols of Armenia and include two (2) gradient effects (rainbow). These UV fluorescent patterns shall include micro-text.
		<b>Polycarbonate data page: title page (page 1)</b>
Req. 66.	Optional	The data page shall integrate the chip and its antenna.
Req. 67.	Required	The data page shall be polycarbonate (100%), with exception for when chip and antenna is integrated in the data page and (or) hinge is not polycarbonate.

Reference	Required / Optional	Description of Technical requirements
Req. 68.	Required	The different layers of polycarbonate that make up the data page shall merge during the lamination process so that any attempt at delamination will destroy the page.
Req. 69.	Required	The title page should incorporate a complex design, including guilloches and fine lines.
Req. 70.	Required	The design of the title page shall illustrate a symbol of Armenia printed with fluorescent inks.
Req. 71.	Required	The title page should include the passport document number pre-personalized.
Req. 72.	Optional	The title page should include the passport document number pre-personalized through the hinge.
		<b>Polycarbonate Data page: Citizen Data page (page 2).</b>
Req. 73.	Required	The data page shall incorporate a complex design comprising at least two (2) visible color gradients (2 "rainbow"), two (2) color gradients visible under UV light (2 "rainbow"), guilloches, fine lines, anti-scan, and micro texts in positive and negative, less than or equal to 250 µm including deliberate errors.
Req. 74.	Required	The data page shall incorporate at least the ePassport symbol below in OVI ink in a location that does not interfere with the reading of other personalized data. 
Req. 75.	Required	The data page shall have tactile elements, some of which include micro-texts.
Req. 76.	Required	The data page shall include personalized information (e.g.: passport number) laser engraved with tactile effect (i.e., passport number).
Req. 77.	Required	The main photo shall be a color photo.
Req. 78.	Required	The data page shall include a secondary image of good size in MLI or CLI.
Req. 79.	Required	The data page will include an OVD type holographic element to secure the main portrait. The design of this OVD will be specific to Armenia.
Req. 80.	Required	The data page shall include infra-red reactive ink (drop-out or anti-stoke).
		<b>Visa pages</b>
Req. 81.	Required	Inside pages shall be 90g / m <sup>2</sup> ± 5% security paper, free of optical brighteners ("UV dull") and made from at least 15% cotton.
Req. 82.	Required	The inside pages shall be printed with inks reactive to attacks by oxidants, acids, bases, and polar solvents, so as to reveal any attempt at forgery.

Reference	Required / Optional	Description of Technical requirements
Req. 83.	Required	The inside pages shall include a complex design, including guilloches and fine lines and at least 2 offset colors gradients ("rainbow") visible, with patterns representing symbols of Armenia (fauna, flora, symbolic monuments, etc.).
Req. 84.	Required	Inside pages should include a page number printed in ink visible on each page, near the edge of the page, and its position should be offset from the previous page to avoid page substitution. Inside pages shall incorporate the page number, printed in fluorescent (under UV) ink.
Req. 85.	Required	The inside pages should incorporate a design printed with fluorescent (under UV) ink. These UV ink patterns shall use the symbols of Armenia and include two (2) gradient effects (rainbow) or more.
Req. 86.	Required	The inside pages shall incorporate colorless fibers under visible light, fluorescent and multi-colored (3 colors) under UV. Each fiber has three colors.
Req. 87.	Required	The interior pages shall incorporate a multi-tone watermark, showing the emblem of Armenia.
Req. 88.	Optional	Each page shall have a unique picture (design), showing different Armenian national symbols (natural landscape, architecture, history, art, etc.).
		<b>Booklet numbering</b>
Req. 89.	Required	The passport number shall be printed in letterpress on page 3 in visible black ink and fluorescent under UV (monochrome).
Req. 90.	Required	The passport number shall be laser punched at the bottom of each inside page, except the polycarbonate data page.
Req. 91.	Required	The passport number shall be perforated using a system which produces conical holes (the width of the holes decreases as the pages progress).
Req. 92.	Required	The passport number shall be laser engraved on the title page.
Req. 93.	Optional	The passport number shall be laser engraved on the title page through the hinge
		<b>Sewing and binding</b>
Req. 94.	Required	The sewing method used to secure the pages to the booklet shall be secure to prevent fraudulent page substitution.
Req. 95.	Required	The binding thread shall consist of three (3) strands of different colors under visible light. At least two (2) strands shall be fluorescent under UV. The fluorescence color under UV should be different for each strand.

Reference	Required / Optional	Description of Technical requirements
		<b>Hinge</b>
Req. 96.	Required	A secure hinge shall secure the polycarbonate data page to the passport booklet.
Req. 97.	Required	The method of securing the hinge shall prevent any attempt to substitute the data page.
Req. 98.	Required	The data page shall be 100% polycarbonate (with exception for when chip and antenna is integrated in the data page and (or) hinge is not polycarbonate), suitable for laser engraving, composed of white and transparent polycarbonate layers.
Req. 99.	Required	The polycarbonate data page shall be attached at the stitching point with the cover and inner sheets with visa pages by means of a hinge that ends at the upper edge of the data page to avoid risk of delamination.
Req. 100.	Optional	The hinge shall be secured by a micro-text chosen by the Authorities.
		<b>Making passport booklets</b>
Req. 101.	Required	The Service Provider shall have at least two manufacturing sites for the production of passports to ensure business continuity.

#### 2.3.4. Specimen and test documents

Reference	Description of Technical requirements
Req. 102.	In addition to the different types of ID1 cards and ID3 documents differentiated during personalization step, the Service Provider shall deliver specimen documents.
Req. 103.	The Service Provider shall prepare and produce specimen folders in order to share the security information among foreign border guard and forensics authorities.
Req. 104.	<p>A specimen folder shall contain the following:</p> <ul style="list-style-type: none"> <li>• One specimen ID card,</li> <li>• One specimen passport,</li> <li>• Brochure depicting security elements of ID card and passport.</li> </ul> <p>The security elements included in the brochure shall be agreed with the Contracting Authority.</p>
Req. 105.	The first 500 specimen folders shall be provided at no cost the Contracting Authority.
Req. 106.	Test certificates shall be provided by the CA, appointed by the GoA.
Req. 107.	Specimens can be produced once the acceptance of the design has been completed on real samples.

Reference	Description of Technical requirements
Req. 108.	The word "SPECIMEN" shall be applied on the documents during the personalization.
Req. 109.	Specimen documents (ID1) are graphically and electronically personalized documents. The Contracting Authority shall submit the fixed dataset for specimens to the Service Provider.
Req. 110.	The Contracting Authority shall be able to order specimens as a folder or separately by Documents type on an ongoing basis.
Req. 111.	Prerequisites to personalize specimen documents are the following: <ul style="list-style-type: none"> <li>• Design acceptance completed,</li> <li>• Chip and software acceptance completed,</li> <li>• Production acceptance completed,</li> <li>• Graphic personalization acceptance completed.</li> </ul>
Req. 112.	Specimen documents shall be delivered in folders with an explanation of each security features of the document allowing the border guards to check and compare the security features on the documents against potential false documents. Content of the sample folder (types of included documents) and the sizes should be agreed with the MFA as a responsible state institution for transferring those to foreign states.
Req. 113.	The folder should contain a USB, which will include electronic version of the printed brochure and other necessary information aligned with MFA.
	<b>Test ID cards</b>
Req. 114.	Test ID cards have the following features: <ul style="list-style-type: none"> <li>• White cards with no security features. Personalization data can be present in case of needed information like PUK/PIN codes,</li> <li>• Electrical personalization is done with a set of data to be agreed during the Setup phase.</li> </ul>
Req. 115.	Citizen test certificates are generated with keys and have the same validity and parameters as the one delivered to the citizen. Test certificates shall be provided by the GoA appointed CA.
Req. 116.	The Service Provider shall provide test documents for the purpose of system development and integration in Armenia.
Req. 117.	The Service Provider shall be responsible for the personalization of test documents.
Req. 118.	The Contracting Authority shall be able to order test documents for ID cards.
Req. 119.	Test ID cards shall be graphically and electronically personalized with the fixed dataset provided by the Contracting Authority. The fixed dataset may include multiple test persons and datasets for the same Document type.
Req. 120.	Test ID cards shall be without artwork. The Service Provider may use other substrate than PC for the ID card test documents.

Reference	Description of Technical requirements
Req. 121.	The test documents shall conform to the chip and software documentation and have the same functionality as the Documents personalized in production environment.
Req. 122.	It shall be possible to order test documents on an ongoing basis. The procedure for ordering test ID cards shall be agreed upon separately with the Contracting Authority.
Req. 123.	Test ID cards ordered prior to the start of the issuance of Documents shall have no cost to the Contracting Authority;
Req. 124.	Test documents ordered after the start of the issuance of Documents shall be subject to the price agreed in the Contract. The Document price will be based on the regular document price indicated in the Proposal.

### 2.3.5. Chip and OS specifications for ID Cards

Reference	Description of Technical requirements
	<b>Cards Chip and OS specifications</b>
Req. 125.	Identity card shall contain 2 certificates, sourced from GoA appointed CA: <ul style="list-style-type: none"> <li>• One for Authentication</li> <li>• One for Signature</li> </ul> Each certificate is based on a key pair generated on board during personalization. The private keys will never be exported from the chip.
Req. 126.	Test ID cards can be produced once the chip specification is approved.
Req. 127.	The ID card chip shall be Common Criteria EAL6 + in compliancy with BSI-CC-PP-0084-2014, having obtained this certificate less than 3 years ago.
Req. 128.	The chip operating system shall be Common Criteria Certified EAL5+ augmented with ALC_DVS.2 and AVA_VAN.5 Open platform including application loading mechanism according to the ANSSI-PP-099-2017-Version3.0.5-Dec 2017
Req. 129.	The operating system shall be compliant with <ul style="list-style-type: none"> <li>• Java card 3.1</li> <li>• Global Platform 2.3</li> </ul>
Req. 130.	The memory space in the chip-OS memory shall offer at least 100kB to store the personalization profile (citizen data).
Req. 131.	Non-traceability of chip characteristics where random chip identifiers reply to each request with a different chip number is mandatory.
Req. 132.	The ID card chip shall support the following cryptographic features: <ul style="list-style-type: none"> <li>• RSA (up to 4096 bits)</li> <li>• ECC (160 bits – 512 bits)</li> <li>• On Board Key Generation for RSA and Elliptic Curve algorithm;</li> </ul>

Reference	Description of Technical requirements
	<ul style="list-style-type: none"> <li>• SHA-224, SHA-256, SHA-384 et SHA-512;</li> <li>• 3DES encryption, decryption, and MAC;</li> <li>• AES encryption, decryption, and MAC calculation (128, 192, 256-bit key length).</li> </ul>
Req. 133.	The operating system shall support SCP03 Secure Channel Protocol
Req. 134.	The Operating System shall be compliant with ISO/IEC 19794-2 (2011) Biometric data interchange formats – part 2 – Finger minutiae data.
Req. 135.	The operating system shall support Match-on-Card (MoC) biometric verification for fingerprints and face. The MoC mechanism shall be evaluated common criteria as part of the OS certification.
Req. 136.	The Operating System shall propose a mechanism enabling to update or securely upgrade the OS and the application in post issuance. This mechanism shall be evaluated common criteria as part of the OS certification.
Req. 137.	<p>The operating system shall provide two independent applications (java Card applet):</p> <ul style="list-style-type: none"> <li>• ICAO applet application compliant with ICAO 9303 Edition 8;</li> <li>• eID applet application for qualified signature and authentication use cases.</li> </ul>
Req. 138.	<p>The ICAO applet shall be certified Common Criteria according to the following protection profiles:</p> <ul style="list-style-type: none"> <li>• BSI-CC-PP-0055 (PP BAC) – certification level: EAL4+;</li> <li>• BSI-CC-PP-0056v1 (PP EAC) - certification level: EAL 5+;</li> <li>• BSI-CC-PP-0068v2 (PP PACE) - certification level: EAL 5+;</li> <li>• BSI-CC-PP-0056v2 (PP PACE with EAC) - certification level: EAL 5+.</li> </ul>
Req. 139.	<p>The chip-OS and ICAO applet shall comply with ICAO layers -6 and -7 and shall be tested by an external lab in compliancy with TR ICAO Part 3 tests and BSI/AFNOR TR03105 Part 3.2 tests for EACv1.</p> <p>The bidder shall provide the external report on compliance.</p>
Req. 140.	The ICAO applet shall support BAC and PACE (GM and IM) reading protocols.
Req. 141.	The ICAO applet shall contain a mechanism that ensures protection of the personalized eID card until it is delivered to the holder (transport of the document, storage, etc.). It shall be able to be activated only at the time of delivery, after requestor authentication.
Req. 142.	Data stored in ICAO applet shall meet the requirements of LDS for Optional Capacity Expansion Technologies, ICAO, Rev 1.7” or “Doc 9303 8th Edition Part 10 Logical Data Structure (LDS) for storage of biometrics and other data in the contactless IC”. Fingerprint information in the Personalization Order shall be forwarded in file format and suitable for writing directly into chip’s LDS DG3 and compliant with BSI TRI-03110.
Req. 143.	<p>The eID applet shall support digital signature and shall be common criteria certified according to the following protection profiles:</p> <ul style="list-style-type: none"> <li>• CEN/EN 419 211-2 (certified under BSI-CC-PP-0059-2009-MA-02) – certification level EAL 5+;</li> <li>• CEN/EN 419 211-3 (certified under BSI-CC-PP-0075-2012-MA-01) – certification level EAL5+;</li> </ul>



Reference	Description of Technical requirements
	<ul style="list-style-type: none"> <li>• CEN/EN 419 211-4 (certified under BSI-CC-PP-0071-2012-MA-01) – certification level EAL5+;</li> <li>• CEN/EN 419 211-5 (certified under BSI-CC-PP-0072-2012-MA-01) – certification level EAL5+;</li> <li>• CEN/EN 419 211-6 (certified under BSI-CC-PP-0076-2012-MA-01) – certification level EAL5+.</li> </ul>
Req. 144.	<p>The eID applet shall be certified eIDAS and referenced on the QSCD European list at eID card field deployment. List available here:</p> <p><a href="https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD">https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD</a></p>
Req. 145.	<p>The eID applet shall support the following services</p> <ul style="list-style-type: none"> <li>• Electronic Signature capability (QSCD) via contact and contactless interfaces;</li> <li>• Key decipherment;</li> <li>• Electronic authentication via contact and contactless interfaces;</li> <li>• PIN and PUK management;</li> <li>• Match on Card user authentication with fingerprint, Face, or Iris biometrics.</li> </ul>
Req. 146.	<p>The eID applet shall embed a mechanism to prevent the usage of the digital services until it is delivered and activated by its owner.</p> <p>The card shall propose a mechanism to secure the delivery of the document to citizen: All the PINs shall be protected and cannot be granted any rights before modifying their values by the citizen.</p>
Req. 147.	<p>The eID applet shall be fully compliant with IAS ECC v1.0 standard.</p>
Req. 148.	<p>The eID applet shall have a mechanism against denial-of-service attack when false PINs are presented up to a certain amount in order to protect the chip against this attack.</p>
Req. 149.	<p>The eID applet shall support changing the PIN codes with the middleware. The eID applet must support resetting the PIN codes using PUK code.</p>
Req. 150.	<p>eID applet must support resetting the PIN codes via secure communication protocol to centralized service (remote reset) in case the citizen loses his PUK and PIN codes.</p>
Req. 151.	<p>Information of the citizen such as name/surname shall be freely readable from the chip through the middleware. Readable citizen data on the chip shall be aligned with GoA during the design phase. The type and the data to be included in the chip will be agree with the Contracting Authority during the design phase of the project.</p>

### 2.3.6. Chip and OS specifications for Passports

Reference	Description of Technical requirements
	<b>Passports Chip and OS specifications</b>
Req. 152.	The passport chip shall be Common Criteria EAL6 + certified. The Operating System shall be Common Criteria EAL5++ certified.
Req. 153.	The contactless electronic component (chip) and its antenna shall be integrated into the polycarbonate data page. The electronic travel document (eMRTD) shall follow the antenna position rules defined in [ISO / IEC 14443-1] and [ISO / IEC 14443-2] for class 1.
Req. 154.	In addition to the biographical data, the image of the face, up to 2 fingerprints and the signature shall be stored in the chip, compliant with BSI TRI-03110.
Req. 155.	Face image shall conform to ISO / IEC 19794-5 and fingerprint images shall conform to ISO / IEC 19794-4.
Req. 156.	The face image size should be stored compressed without significant loss of image quality.
Req. 157.	Fingerprint images should be stored compressed using WSQ compression.
Req. 158.	The ICAO applet shall support BAC and PACE (GM and IM) reading protocols.
Req. 159.	The ICAO applet shall contain a mechanism that ensures protection of the personalized passport until it is delivered to the holder (transport of the document, storage, etc.). It shall be able to be activated only at the time of delivery, after requestor authentication.
Req. 160.	The ICAO applet shall be certified Common Criteria according to the following protection profiles: <ul style="list-style-type: none"> <li>• BSI-CC-PP-0055 (PP BAC) – certification level: EAL4+;</li> <li>• BSI-CC-PP-0056v1 (PP EAC) - certification level: EAL 5+;</li> <li>• BSI-CC-PP-0068v2 (PP PACE) - certification level: EAL 5+;</li> <li>• BSI-CC-PP-0056v2 (PP PACE with EAC) - certification level: EAL 5+.</li> </ul>
Req. 161.	In order to streamline border crossings, the travel application shall allow secure reading of biographical and biometric data (2 fingerprints) in a maximum of 4 seconds.

### 2.3.7. Middleware for ID card

Reference	Description of Technical requirements
Req. 162.	Software (middleware/libraries, desktop application and browser integrations) supporting the usage of eID Applet via contact and contactless (NFC) interface must be delivered.
Req. 163.	The card middleware shall support MS Windows, MacOS, Linux, Android, iOS \operating systems for desktop computers, servers and smartphones.
Req. 164.	The middleware shall be compliant with the following standards: PKCS#11 for Windows, Linux, Mac, Minidriver for Windows and Crypto Token Kit (CTK) for MacOS.
Req. 165.	The Vendor at all times of the contract term shall provide the smooth operation and updates of the software for all supported operating systems and browsers (Firefox, Google chrome, Apple Safari).

Reference	Description of Technical requirements
Req. 166.	The middleware shall offer interfaces to perform fingerprint match-on-card.
Req. 167.	The middleware shall offer interfaces to perform facial match-on-card.
Req. 168.	The desktop application shall provide at least the same functionality as the current Armenian National ID card middleware (CryptoCard Suite), minimally including: <ul style="list-style-type: none"> <li>• seeing information about the keys and certificates</li> <li>• seeing the information file</li> <li>• changing PIN(s) using known PIN(s)</li> <li>• unblocking/changing PIN(s) using PUK(s)</li> <li>• activating PIN(s) (if applicable)</li> </ul>
Req. 169.	The desktop application shall have the modular architecture to enable support of other types of chips in the future, as well as current ID cards issued before 15th of February 2023. The current ID card chips support PKCS#11 interface.
Req. 170.	The desktop application shall provide a possibility to add certificates to the operating systems trust stores.
Req. 171.	The middleware shall offer an interface to interact with the card on web application. A common JavaScript API for desktop and mobile shall be provided. Most common browsers (such as: Edge, IE, Chrome, Safari, Firefox) shall be supported.
Req. 172.	The card information reading software shall be provided with the possibility to read the data stored in ICAO Applet and present it in a machine-readable format.
Req. 173.	The card information reading software shall be provided with the possibility to read the data stored in information file stored on chip and present it in a machine-readable format.
Req. 174.	The software shall ensure multilingual interface including Armenian, English, and Russian.
Req. 175.	The Source Code (excluding middleware/libraries), documentation, and all rights of the software (excluding middleware/libraries) shall be passed to GoA after the implementation phase in respect of the requirements in Annex 5 and Annex 6.

## 2.4. Requirements for the Identity and Document Management Information System

### 2.4.1. Non-functional requirements for IDMIS

Reference	Required / Optional	Description of Technical requirements
		<b>General requirements</b>
Req. 176.	Required	The system shall be designed to meet up to 20% of growing needs in terms of document volume, without impacting the existing architecture.
Req. 177.	Optional	The system shall be flexible and be based on open standards. The solution shall comply with the “Open Standard Identity API” (OSIA) standard. The Service Provider will have to present their system architecture showing compliance with the OSIA architecture model.
Req. 178.	Required	Human Interfaces shall be available in Armenian and in English.
Req. 179.	Required	Source Code for all software components, incl. IDMIS software components, ID card and passport chip, OS and ID card middleware, must be stored in the Escrow account for the duration of the Contract (for more details please refer to Annex 6). Requirements related to storing Source Code in the Escrow account shall comply with Annex 6.
		<b>System user and rights management requirements</b>
Req. 180.	Required	The solution shall manage the personal and professional details of each internal user: name, address (office, residence), contact information (mobile, e-mail, landline, etc.), login, authorized connection slots, connection terminal and authorized functions.
Req. 181.	Required	Access to the system, modules and functions shall be controlled by specific rights. Different rights shall be configurable for different roles. Each role shall group together a set of rights to access and launch certain system tasks. Roles shall be customizable in accordance with the requirements of the Contracting Authority.
Req. 182.	Required	The user (operator, administrator, etc.) will automatically receive all the predefined rights for the group to which he belongs.
Req. 183.	Required	All transaction must be traceable to the specific user who permed the actions.
Req. 184.	Required	Both Contracting Authority and Service Provider should be able to manage user rights of their employees respectively.

Reference	Required / Optional	Description of Technical requirements
Req. 185.	Required	Contracting Authority shall have access and right to audit all user and rights configuration and transaction log.
		<b>Security and data protection requirements</b>
Req. 186.	Required	The Service Provider shall grant a state-of-the-art security of its service (except for ABIS), ensuring protection against outside and inner circle attacks, intrusions, and internal unauthorized use. It is the responsibility of the Service Provider to ensure the right level of security and data protection during the contract period.
Req. 187.	Required	Service provider shall meet the Minimum Security Principles stipulated in the Annex No. 4.
Req. 188.	Required	Measures shall be taken to address various types of cyberattacks against production facilities, such as: <ul style="list-style-type: none"> <li>• Viruses and other malware, compatible with the computer installations and production machines.</li> <li>• DDOS attacks through on-line application channels and online services exposed by production and issuance systems.</li> </ul>
Req. 189.	Required	The data storage shall grant the data confidentiality.
Req. 190.	Required	Detection of integrity breaches of the combined application data shall be monitored. The detection of an integrity breach is considered as a security incident that shall stop the production of personalized documents.
Req. 191.	Required	The system shall provide a full, tamperproof audit trail. The solution shall allow traceability of all operations through functional and technical logs on all modules in the solution. The logs can be used for security audit and reporting purposes. Contracting Authority shall have full unlimited access rights to system logs.
Req. 192.	Required	The system shall provide the possibility to prevent modification, change and / or deletion of any data-on-data base level, except specific use cases defined in the IDMIS design documentation aligned with Contracting Authority.
Req. 193.	Required	Biometric and personal data both in transit and at rest shall be encrypted with secure protocols and algorithms. If encryption is not possible, the Service provider shall align reasoning with the Contracting Authority during the design phase.
Req. 194.	Required	Any communication between different networks shall be encrypted with secure protocols and algorithms.
Req. 195.	Required	The system and its data should only be accessible only to authorized staff on per role basis (except for the public website and online service).

Reference	Required / Optional	Description of Technical requirements
Req. 196.	Required	The availability of data on persons holding diplomatic (service) passport and accredited in RA foreign diplomats (consular and administrative workers), as well as employees of international organizations should be restricted solely to the appointed GoA employees.
Req. 197.	Required	The system shall ensure data protection policies enforcement (e.g., allow deletion of data after agreed period, provide logs for accessing citizen personal data, etc.).
Req. 198.	Required	The system must maintain data minimization principle, ensuring only data that is required for issue of identity and travel documents is collected.
Req. 199.	Required	All biometric data shall be deleted from the system components other than Biometric data and document registry not later than in 48 hours. Time to delete biometric data shall be a configurable parameter.
Req. 200.	Required	The system shall provide solution for performance and incidents monitoring, statistics, and reporting.
Req. 201.	Required	The service provider shall propose an incident reporting management organization during the setup of the project Incident reporting plan shall be approved by the Contracting Authority during the design phase.
Req. 202.	Required	Security measures shall be also part of the development, testing and production environment.
Req. 203.	Required	Access roles for the DEV, Test and Prod environments for development support, routine maintenance and monitoring must be separated using an identity access management solution that controls authentication and authorization to these environments.
Req. 204.	Required	In addition to ISO 9001 and ISO 27001 certifications, the solutions implemented must not carry over any residual risk that may affect the performance or may expose the services to vulnerabilities which may in turn affect the quality of services rendered.
		<b>Back up and archiving</b>
Req. 205.	Required	There shall be a possibility to make backup copies for all stored data both in the operating (located in the main data center) and non-operating (located in the DRS, after it is activated) System, while complying with all the System performance requirements specified in this document and not disturbing the work with the System.
Req. 206.	Required	Backup and archived datasets shall be encrypted and secured to the same level as operational datasets are secured.
Req. 207.	Required	System administrators shall be able to set automatic backup copying and configure frequency, storage location (logical disk, remote stations, etc.), categories of documents/ data to be backed up, also to execute the backup of the entire System.

Reference	Required / Optional	Description of Technical requirements
Req. 208.	Required	System users shall be able to initiate System data restoration procedure from backup copy. After restoring the data, data integrity shall be ensured and applied thereafter, i.e., measures for automatic verification for ensuring data correctness and integrity during data restoration shall be implemented in the System.
Req. 209.	Required	The System shall have a backup copying and restoration log. There shall be a possibility to review and print the log.
Req. 210.	Required	In addition of the regular Back Up Policy that will be operated by the Service provider to run the service and based on the same process (details & period that will be agreed after signing the contract with the winning vendor), the Service provider shall provide a backup copy of all the administrative data stored in the System databases to the Contracting authority. However, Service provider retains the right to keep these administrative data in the original location in the System databases.
Req. 211.	Required	The System shall provide the possibility to archive inactive data, by putting them in a different architectural level of the database, in order to improve System performance. Service provider shall specify and confirm the detailed rules on the identification and archiving of inactive data during the detailed analysis and design phase.
Req. 212.	Required	If necessary, it shall be possible to restore the data transferred for long-term storage from the archive data warehouse and viewed in forms (without the possibility of editing).
Req. 213.	Required	The System shall provide the possibility to automate data archiving processes and archived data storage management.
Req. 214.	Required	The System shall provide the possibility to select and create a data list for automatic archiving.
Req. 215.	Required	The System shall provide the possibility to prevent modification, change and/ or deletion of archived data.
Req. 216.	Required	The System shall provide the possibility to set individual archiving settings for any data category.
Req. 217.	Required	The System shall provide the possibility to specify and change the periodicity and period for data archiving.
Req. 218.	Required	From the archived data the System shall provide the possibility to generate detailed reports.
Req. 219.	Required	The System shall provide the possibility to view archived data without the need for any additional software.
Req. 220.	Required	The data of deceased persons shall be archived (among other data to be archived).
Req. 221.	Required	Cryptographic keys used during the project and used for the operations (personalization and post issuance) shall be shared and stored with the Contracting Authority.

## 2.4.2. Functional requirements for IDMIS

Reference	Required / Optional	Description of Technical requirements
		<b>General requirements</b>
Req. 222.	Required	<p>The Service Provider shall provide a comprehensive solution and services, covering the entire document lifecycle from citizen request to issuance and delivery of their biometric passport and ID card. The various modules/functionalities of the system shall be integrated in order to offer a fully automated service comprising, but not limited to the following functions (described separately in following chapters):</p> <ol style="list-style-type: none"> <li>1. Citizen eService application (web portal)</li> <li>2. Enrolment solution</li> <li>3. Identity management and document issuance solution</li> <li>4. Biometric data and document registry</li> <li>5. Automated Biometric Identification Solution (ABIS)</li> <li>6. Public key infrastructure</li> <li>7. On-site queuing management solution</li> <li>8. Reports and statistics solution</li> <li>9. Integrations with external data sources</li> </ol>
Req. 223.	Required	All hardware and software necessary to perform requirements below shall be included in the tendered proposal.
Req. 224.	Required	Enrolment stations shall be set up across the country and in foreign missions (consulates and embassies).
Req. 225.	Required	Customer experience in both facilities set in the country and in foreign missions (except the queuing system, that are not deployed abroad) shall not differ and meet the same specifications.
Req. 226.	Required	<p>Service provider must equip a dedicated space in the main office of the Migration Service with equipment necessary for remote monitoring of all facilities in Armenia (enrolment, personalization, data center, DRS) real time, incl. but not limited to (final list and specifications must be agreed with Contracting Authority during the design phase of the project):</p> <ol style="list-style-type: none"> <li><b>1. Control consoles:</b> equipment to allow the operator to adjust the surveillance system's functions, such as switching between video feeds and controlling and changing camera settings.</li> <li><b>2. Storage units:</b> after capturing footage, CCTV surveillance cameras must transmit signals to the security camera recorders for saving and replaying key moments.</li> <li><b>3. Displays:</b> display system that shows all the videos captured by different cameras from distinct sources.</li> <li><b>4. Network equipment:</b> routers, switches, and servers to allow video feed to be transmitted and managed across a network.</li> </ol> <p>The Service Provider shall provide the necessary infrastructure for real-time video surveillance of the various premises under the operational responsibility of the service provider (as described</p>



Reference	Required / Optional	Description of Technical requirements
		above), but the storage of these videos and their re-viewing remains under the responsibility of the Contracting Authority.
		<b>Citizen eService application (web portal)</b>
Req. 227.	Required	Citizen eService application is a public web portal dedicated to the pre-enrolment and follow-up eServices and information provision on issuance of the Identity and travel documents.
Req. 228.	Required	This web portal shall provide a user-friendly interface for the smartphone, tablet or computer.
Req. 229.	Required	This web portal shall be adapted to the graphic charter of the Government portals (design guidance to be provided by the Contracting Authority) and should also be accessible via active link from the government web pages/platforms (specified by the Contracting Authority in the design phase).
Req. 230.	Required	For online service that require user authentication, external users (applicants) must be authenticated via Governmental gateway.
Req. 231.	Required	The web portal shall allow applicants to book an appointment for a face-to-face biometric enrolment, personalized document pick up, or other service available in the enrolment facilities (E.g., PIN change): <ul style="list-style-type: none"> <li>• The applicant shall be able to change the time of the appointment.</li> <li>• Online appointment booking functionality shall allow to see availability and book appointment in different enrolment stations across all territory of Armenia.</li> <li>• Once the request has been validated and the appointment has been set, the portal shall generate proof of this validation which will serve as a reference at the time of biometric enrolment.</li> <li>• Back-office software for managing the available timeslots shall be provided together with the solution.</li> </ul>
Req. 232.	Required	The web portal shall allow applicants to request for a new ID document (first time and renewal), incl. but not limited to filling in a form with their biographical data, uploading documents necessary for the application, e.g., breeder documents (for citizens below the age of 18 - a written consent of the parents and the child (if the applicant does not have a passport of a citizen of the Republic of Armenia); appropriate medical document, if the citizen wishes to record the data on blood group and rhesus in the ID card, etc.), etc.
Req. 233.	Required	The web portal shall allow applicants to pay their fee online in (via payment card and local payment service providers): <ul style="list-style-type: none"> <li>• Solution shall allow applicants to initiate payment</li> <li>• Solution shall be able to receive and manage payment status information received from payment card and local payment service providers (including but not limited to recall and dispute processes, incorrect amounts paid, etc.)</li> <li>• Regular payment shall be collected to the escrow account</li> </ul>

Reference	Required / Optional	Description of Technical requirements
		<ul style="list-style-type: none"> <li>Fast-track service payments shall be processed by the Service Provider, but the solution shall allow splitting payment to different accounts according to the set rules: part of the payment (additional fees for fast-track service, exceeding regular document price) shall be directed to the Service provider account, another part (regular document price) – to the escrow account.</li> <li>Credit risk shall be managed by the Service Provider</li> <li>Back-office solution shall provide functionality for automatic payment information reconciliation with state treasury information system</li> </ul>
Req. 234.	Required	The web portal shall allow applicants to report loss or theft of an ID document.
Req. 235.	Required	The web portal shall allow applicants to monitor the status of their ID documents requests / document issuance process documents from enrolment to the availability for issuance and notify citizen on the status change via preferred channel.
Req. 236.	Required	The web portal shall ensure that data available in the registries or system (e.g., Population registry) must be used to check validity of the data provided by the citizen.
Req. 237.	Required	The web portal must use secured https protocol.
		<b>Enrolment solution</b>
Req. 238.	Required	<p>To cover the enrolment needs throughout the country and in overseas missions, fixed and mobile enrolment stations shall be deployed in accordance with paragraph 2.2.1 “Requirements for enrolment facilities (service points)”. Even if hardware configuration is different, the functionality and provided security level of the fixed and mobile stations shall be equivalent.</p> <p>A list of actual service points and their historical workload is listed in “Annex No. 1: Data about issued document volumes, enrolment / customer service facilities operated in Armenia and in foreign missions”.</p>
Req. 239.	Required	<p><b>Enrolment facilities in Armenia</b></p> <p>Enrolment equipment necessary for the end-to-end enrolment service (combination of desktop or enrolment booth and mobile units (dedicated to reach remote location or vulnerable groups)) shall be installed in at least:</p> <ul style="list-style-type: none"> <li>one (1) or up to three (3) centralized facilities shall be established in Yerevan (number of facilities operated in Yerevan cannot exceed three (3)).</li> <li>At least twelve (12) in the regions outside Yerevan.</li> </ul> <p>Actual number of workstations (combination of fixed and mobile stations) shall be decided by the Service provider, considering SLAs</p>

Reference	Required / Optional	Description of Technical requirements
		<p>set in this document, expected service demand and the designed geographical network of service point.</p> <p>Service provider will propose an optimal number of workstations in Armenia to be able to meet required service level based on actual demand (based on the estimated service volumes provided in Annex No. 3).</p>
Req. 240.	Required	<p><b>Enrolment facilities in foreign missions</b></p> <p>Enrolment equipment necessary for end-to-end enrolment service (combination of desktop or enrolment booth and mobile units (dedicated to reach remote location or vulnerable groups)) shall be installed in 61 service points in foreign countries with Armenian consulates / embassies and MFA office in Yerevan (current 54, 7 to be opened in 2024) (price must be included in the Financial Proposal).</p> <p>It is expected that Service Provider will deliver and set-up 67 fixed enrolment stations (out of which 2 in the MFA office in Yerevan) and 2 mobile stations to be operated by Ministry of Foreign Affairs in embassies and consulates (price must be included in the Financial Proposal).</p> <p>Additional 15 service points in foreign missions may be opened in the upcoming 11 years (not part of the initial Financial Proposal).</p> <p>Please note: for the enrolment solutions to be deployed in foreign missions that exceed currently foreseen 69 enrolment stations (67 fixed and 2 mobile), the financial proposal must include the additional price for a single enrolment station. When new service station is planned to be opened, additional purchase order shall be signed.</p>
Req. 241.	Required	<p>The operators shall authenticate to the system in a secured way based on digital certificate of their ID card.</p>
Req. 242.	Required	<p>Enrolment stations shall be able to retrieve the information provided during pre-enrolment and capture the biometric data of the applicant (portrait, fingerprints).</p>
Req. 243.	Required	<p>Enrolment stations shall enable the required supporting documents to be scanned, all in accordance with ICAO standard 9303, 8th edition and the regulation of Armenia.</p> <p>Compliance to the ICAO Doc 9303 shall be checked automatically for all the input document / data.</p>
Req. 244.	Required	<p>The enrolment solution shall work in online or offline mode. The enrolled data shall be transmitted to the data center securely through the network. A temporary or persistent disconnection from the network should not impact the enrolment process or the integrity of data already captured. The enrolment solution shall manage data synchronization with the data center when the network connection is restored.</p>

Reference	Required / Optional	Description of Technical requirements
Req. 245.	Required	<p>Fixed and mobile enrolment stations shall allow entry, correction or capture of the following data:</p> <ul style="list-style-type: none"> <li>• Alphanumeric biographical information,</li> <li>• Portrait,</li> <li>• Prints of the two fingers flat,</li> <li>• Signature,</li> <li>• Scan of supporting identity documents.</li> </ul>
Req. 246.	Required	<p>The stations will also be equipped with a printer, scanner, a camera, a passport and card reader and necessary accessories/equipment (tripod for the camera, barcode reader, backdrop, connectors, el. document signature pads, payment card readers, cash collection/deposit machines, etc.).</p>
Req. 247.	Required	<p>Service provider upon the request of the Contracting Authority shall be able to offer not only regular enrolment stations, but also all-in-one solution that may be implemented in all or part of the enrolment facilities.</p> <p>An all-in-one solution for enrolment station equipment refers to a unified system that combines multiple biometric and administrative functions into a single, cohesive unit (incl. biometric data capture, data processing and management, identity verification, signature capture, payment handling and other), enabling physical enrolment in full autonomy.</p>
Req. 248.	Required	<p>Service provider shall ensure, to the extent possible according to relevant standards, paperless process (no physical documents stored, signing the documents through tablets / machines instead of paper application forms).</p>
Req. 249.	Required	<p>In case when applications are handled by paper, the Service Provider shall ensure digital archiving of the applications. Digital records retention policy requirements (access, availability, deletion date etc.) shall be agreed with the Contracting Authority during the design phase.</p>
Req. 250.	Required	<p>Service provider shall ensure different payment methods:</p> <ul style="list-style-type: none"> <li>• Remote online and offline payment via credit card, bank and (or) other payment service providers,</li> <li>• Via credit/debit card in the service station (at the counter).</li> </ul>
Req. 251.	Required	<p>In cases when mobile stations are used, mobile enrolment stations shall include a battery capable of operating for 8 hours.</p> <p>The components of the mobile station shall be integrated into a transport case resistant to shocks, water, and dust. This case shall not only protect the equipment during transport, but also allow easy deployment of the station.</p>

Reference	Required / Optional	Description of Technical requirements
Req. 252.	Required	The operator shall be able to monitor, in real time and on the screen of the enrolment system, the photo to capture.
Req. 253.	Required	Biometric data compression formats shall comply with international standards, in particular: <ul style="list-style-type: none"> <li>• FBI Wavelet Scalar Quantization (WSQ) Image compression standard for fingerprints of 500dpi.</li> <li>• ISO 10918-1, 1994. Joint Photographic Experts Group (JPEG).</li> <li>• Compression standard for continuous tone images (photography).</li> </ul>
Req. 254.	Required	For the camera and he captured photo the following requirements shall be met: <ul style="list-style-type: none"> <li>• ICAO standard and ISO 39794-5 and the enrolment station shall control it,</li> <li>• ISO / IEC 19794-5 and ICAO 9303, 8th edition portrait quality as well as requirements for camera-to-subject distance,</li> <li>• The enrolment system shall incorporate an automatic cropping function for the photo.</li> </ul>
Req. 255.	Required	For the fingerprint readers, the following requirements shall be met: <ul style="list-style-type: none"> <li>• FBI IQS and ISO 19794-4 compliance for fingerprint quality,</li> <li>• Capture quality of 500 dpi with 256 grey levels,</li> <li>• FAP10 capture zone (full fingerprint images, not just a partial spot),</li> <li>• Fingerprint images must be compressed using the WSQ algorithm (FBI/NIST standard), RAW or ISO 19794-4 format,</li> <li>• Encryption of both image and template data from the device to the computer, ensuring secure transmission.</li> </ul>
Req. 256.	Required	The enrolment system should incorporate real-time quality control, indicating to the operator whether the captured fingerprints are of sufficient quality. The system shall guide the operator by recommending in particular another acquisition if the minimum quality threshold is not reached and display the NIST Fingerprint Image Quality (NFIQ) score.
Req. 257.	Required	The enrolment system shall make it possible to manage fingerprint capture exceptions (bandaged, amputated, damaged fingers, etc.).
Req. 258.	Required	Data stored on the enrolment station shall be encrypted by the enrolment solution. The enrolment system shall also secure by encryption the submissions of biographical and biometric data to the Identity management and document issuance system.
		<b>Identity management and document issuance solution</b>
Req. 259.	Required	The global identity management and document issuance solution shall be based on an integration platform that links the different modules of the solution.

Reference	Required / Optional	Description of Technical requirements
		This platform shall make it possible to manage the flow of data between the various registries / applications, from enrolment to delivery of the document (enrolment, deduplication, identity management, personalization, quality control, secure delivery).
Req. 260.	Optional	Integration platform that links the different modules of the identity management and document issuance solution and its interfaces shall comply with OSIA specifications to allow easy future evolution.
Req. 261.	Required	This solution shall process any new identity document applications by checking its validity and upon successful identity verification, feed or update the Biometric data and document registry accordingly.
Req. 262.	Required	The solution shall support vetting process and allow back-end employees to approve or reject the application and grant approval to issue the document, validate information with other GoA systems (e.g., population register) and check manually the biometric mismatches (comparing 1-N fingerprints and portrait) the system is highlighting.
Req. 263.	Required	It should not be possible to form a passport by one official person on the level of software solution and should be executed by the approval of at least one level higher supervisor as an internal control mechanism.
Req. 264.	Required	The tools dedicated to biometric verification solution shall be based on advanced biometric comparison features (image enhancement, display of minutiae, overlay of portraits, etc.) through a user-friendly interface.
Req. 265.	Required	The biometric verification solution shall make it possible to juxtapose the candidate's biometric data with those of the corresponding records in the database, in order to compare the portrait and the fingerprints, one by one. For the portrait, this support tool should automatically superimpose the two photos.
Req. 266.	Required	<p>The solution shall integrate an investigation station that allows examination of the applicant's file as a whole. When a biometric duplicate is confirmed, this tool shall display, in a user-friendly way, the candidate's biometric, biographical, and additional information (supporting documents) as well as those of the records whose biometrics match.</p> <p>The Documents and biometric data registry / database will be updated based on the findings of this investigation.</p>
Req. 267.	Required	The solution should allow prioritize certain applications and form print order in a prioritized mode (e.g., diplomats accredited in Armenia should be executed in prioritization mode).

Reference	Required / Optional	Description of Technical requirements
Req. 268.	Required	The solution shall manage and track the life cycle of passports and cards application and document status (e.g., Created, Approved, Not approved, Dispatched, Received, Secured, Locked, Terminated, Revoked, etc.), so that it can report status to the applicant and document status through the web application portal website to the applicant.
Req. 269.	Required	The applicant (incl. those who in Armenia and in foreign missions, also foreign diplomats accredited in Armenia) should be informed by SMS when their identity document is available.
Req. 270.	Required	The service points shall deliver the passports and cards. For this, the station shall allow biometric authentication of applicants to enable a full data matching and chip functionalities.
Req. 271.	Required	The Service Provider shall propose a solution to enable the chip of the document to be activated only after successful biometric authentication of the applicant.
Req. 272.	Required	Solution shall enable post-issuance services for ID document such as PIN unlock /change, termination of lost documents, revocation of certificates in case of lost documents, etc..
Req. 273.	Required	<p>Solution shall enable digital storing and archiving of all correspondence and documentation (applications/forms, complains, letters, etc.) collected and generated during the enrolment and other customer service interactions. Both digital and physical received documents must be scanned, stored and archived.</p> <p>System shall allow review and printing of stored and scanned document for authorized system users.</p> <p>Document archiving / retention policy and rules must be defined and aligned with GoA during the design phase of the project.</p>
		<b>Documents and biometric data registry / database</b>
Req. 274.	Required	<p>The solution shall enable managing information about documents issued to citizens and their biometric data, incl. but not limited to:</p> <ul style="list-style-type: none"> <li>• Alphanumeric biographical information,</li> <li>• Portrait,</li> <li>• Prints of the [two] fingers flat,</li> <li>• Signature,</li> <li>• Scan of supporting identity documents.</li> </ul> <p>Complete list of biometric and document data shall be agreed with the Contracting Authority during the design phase/</p>
Req. 275.	Required	The Service Provider tender shall either perform a migration of the existing biometric data into a new biometric database or ensure integration interface with legacy biometric data registry.

Reference	Required / Optional	Description of Technical requirements
Req. 276.	Required	The database shall have the capacity to store a minimum of [10] million records including all data relating to the identity of applicants (biographical and biometric information, conservation of the history of biometric data over the course of their life) as well as administrative and technical data (functional and technical logs, etc.).
Req. 277.	Required	All database data shall be stored encrypted in logical structure based on the possibilities of products used (e.g., Oracle) as well as adhering to requirements of applicable regulations (e.g., eIDAS).
Req. 278.	Required	The solution shall be implemented in the data center provided by the GoA and operated / maintained by GoA employees.
Req. 279.	Required	For each data request the solution shall record the proof of a legitimate cause for the request.
		<b>Automated Biometric Identification Solution (ABIS)</b>
Req. 280.	Required	The Service Provider shall implement an integrated Automated Biometric Identification System (ABIS), including the necessary hardware, software, and database. It shall be able to process the fingerprints of the [2] fingers and the portrait.
Req. 281.	Required	The ABIS covers 3 tasks: <ul style="list-style-type: none"> <li>• Registration of data during application,</li> <li>• Verification Biometrics 1:1,</li> <li>• The search with fingerprints for identification.</li> </ul>
Req. 282.	Required	Search functions of the system are used by: <ul style="list-style-type: none"> <li>• The Identity management and document issuance solution,</li> <li>• The border guard,</li> <li>• The police.</li> </ul>
Req. 283.	Required	The ABIS shall provide biometric authentication (type 1: 1 request) and biometric identification (type 1: N request) services by comparing the biometric data of the requester with those contained in the database.
Req. 284.	Required	The ABIS shall be compatible with the ISO 19794-1, -2, -3, -4, -5, WSQ and JPEG / JPEG 2000 formats.
Req. 285.	Required	The system shall identify and code the minutiae.
Req. 286.	Required	The ABIS shall operate in "multimodal" or "biometric fusion" mode to improve search accuracy and performance by combining multiple biometrics, including fingerprints and portrait, in a single request.
Req. 287.	Required	The solution shall be sized to perform multimodal deduplication of 10 fingerprints and one face in a database that can hold up to [10] million records up to [6,000 requests] daily during business hours [8 hours].



Reference	Required / Optional	Description of Technical requirements
Req. 288.	Required	The expected response time for each multimodal (1: N) deduplication request in a base of [10 million] records shall be less than or equal to 10 seconds.
Req. 289.	Optional	The ABIS shall comply with "Open Standards Identity API" (OSIA) standards, in order that standard APIs are accessible to external systems (public administrations, private entities, etc.).
Req. 290.	Required	The ABIS shall save the history of transactions in functional and technical logs (multiple enrolments, deletion of fraudulent identity following deduplication, etc.).
Req. 291.	Required	The Service Provider shall rely on facial recognition algorithms submitted to "NIST FRVT ongoing" whose NIST report of March 2021 is available at: <a href="https://pages.nist.gov/frvt/html/frvt1N.html">https://pages.nist.gov/frvt/html/frvt1N.html</a>
Req. 292.	Required	The Service Provider shall have to rely on fingerprint recognition algorithms submitted to NIST FpVTE. Provide the evaluation report.
Req. 293.	Required	<p>Before personalization, the fingerprints will be matched against the ABIS during application validation process by the Migration Service. It is performed in the case of an initial security issue and includes a comparison of the fingerprint and/or facial image collected for the issuance of the document with all the biometric data stored in the biometric database to confirm that no other security document has been issued to the same person.</p> <p>Those checks will be carried out by the Migration Service, at premises appointed by GoA before the ID documents are personalized and without the presence of the Service Provider.</p> <p>In case of any mismatch on one of the registers or ABIS or a hit on the list of wanted persons an employee of the Armenian Government takes over the case and executes an investigation. The identity information from the National Register of Citizens is always leading in case of doubt about the correctness of identity details.</p> <p>The verification process may not be influenced by human intervention. Only exception is for technical support in which case four eyed controlled access shall be applied combined by temper proof logging.</p>
Req. 294.	Required	<p>The biometric verification/identification (ABIS) system shall ensure:</p> <ul style="list-style-type: none"> <li>• Performance and processing of multiple biometric transactions as follows: <ul style="list-style-type: none"> <li>○ 1:1 Verification ≤ 2sec,</li> </ul> </li> </ul>

Reference	Required / Optional	Description of Technical requirements
		<ul style="list-style-type: none"> <li>○ 1:N Identification ≤ 10 secs.</li> <li>• Accuracy and reliability at a percentage: <ul style="list-style-type: none"> <li>○ True Match Rate (TMR) of at least 99.9%,</li> <li>○ FAR Fingerprint Recognition &lt;0.01%,</li> <li>○ FRR Fingerprint Recognition &lt;1%,</li> <li>○ FAR Facial Recognition &lt;0.1%,</li> <li>○ FRR Facial Recognition &lt;3%</li> </ul> </li> <li>• Not affected by features such as image rotation</li> </ul> <p>These requirements shall be certified during the acceptance / delivery phase of the project through the performance of the necessary acceptance tests. Test plan completion report must be provided, specifying test scenarios and pass results. Service Provider must be able to demonstrate successful competition of applicable test scenarios upon request in both testing and production environments.</p>
Req. 295.	Required	For each request the solution shall record the proof of a legitimate cause for the request.
<b>Personalization solution</b>		
Req. 296.	Required	The personalization solution shall include the hardware and software elements necessary for graphic and electrical personalization of all Identity documents of this specification.
Req. 297.	Required	The document personalization solution shall cover the graphical and electrical personalization of the passports and cards (laser engraving, secure chip encoding) and integrate a unitary quality control and packaging for handover at the distribution sites.
Req. 298.	Required	The same software solution shall manage passports and cards personalization processes. It shall be able to pilot several personalization machines in parallel.
Req. 299.	Required	The solution shall be sized to absorb the quantities of documents and production peaks indicated during a daily production shift of [7] hours.
Req. 300.	Required	The personalization solution shall integrate with the Identity management and document issuance solution in order to collect and process any new validated application for card and passport. It shall also interface with the eMRTD PKI solution (provided by the Service Provider) and with the citizen PKI (provided by the CA appointed by GoA).
Req. 301.	Required	The solution shall keep track of all administrative actions (author, date, etc.) to enable security audit.

Reference	Required / Optional	Description of Technical requirements
Req. 302.	Required	The solution should allow execute certain print orders in a priority manner (e.g., diplomats accredited in Armenia should be executed in prioritization mode).
Req. 303.	Required	All personalization processes shall adhere to the highest security standards to ensure data security and privacy.
Req. 304.	Required	The personalization solution shall include a quality control module that will verify proper execution of the physical (position and quality) and electrical (full read test) personalization operations. The quality control module shall display the test results through a user-friendly graphical interface, showing compliance and non-compliance.
Req. 305.	Required	If quality control rejects document personalization for non-compliance(s), following validation by the Quality Control operator, the system shall allow automatic launch of a new personalization process.
Req. 306.	Required	The personalization solution shall allow ID Cards and passports to be stored in boxes according to their place of delivery, in order to facilitate shipment to delivery sites. Boxes and each ID card individually shall be identified using labels to enable track and trace of the shipments to delivery sites
Req. 307.	Required	The personalization solution shall include an inventory management module with the following functionalities: <ul style="list-style-type: none"> <li>• Keeping an inventory of blank documents,</li> <li>• Safekeeping of blank documents shall be subject to double biometric controls access,</li> <li>• Visualizing the stock of all blank documents with the possibility to generate reports for the Contracting Authority audits.</li> <li>• Having an early warning system for critical stock levels by type of document.</li> </ul> A report will be produced each month to reflect the volume of production and the stock.
Req. 308.	Required	The Service Provider shall organize the personalization technique and process in such a manner that labor safety and hygiene of the document personalization process is guaranteed.
Req. 309.	Required	The Service Provider shall interface with the CA that the Contracting Authority will appoint in order to ask for and receive the ID card certificates.
Req. 310.	Required	Up to 3 changes in the CA shall be included in the Contract and final price. Any changes above 3 will be handled by change request process.

Reference	Required / Optional	Description of Technical requirements
Req. 311.	Required	The solution shall manage the acceptance or rejection of a document or batch of documents and transmit this status to the Identity management and document issuance solution.
Req. 312.	Required	The Service Provider shall ensure personalization solution does not store any sensitive data: all sensitive data (personal data of the citizens) must be deleted from the personalization system and respective databases immediately after production of the identity document is completed.
		<b>ICAO/EAC Public key infrastructure</b>
Req. 313.	Required	The PKI system shall comply with ICAO standard 9303, 8th edition, regarding management of the eMRTD PKI (PKI ICAO and PKI EAC), in particular the cryptographic algorithms and management of the life cycle of the keys, the contents of the certificates and revocation lists (CRLs), distribution mechanisms for certificates and revocation lists etc.
Req. 314.	Required	The eMRTD PKI system shall ensure complete management of the keys and certificates used to sign passport data during personalization and allow their verification at checkpoints (Passive Authentication). It should address all aspects of creating, managing, and revoking keys and certificates and associated policies, in a flexible, user-friendly manner.
Req. 315.	Required	The system shall integrate a national PKD with a connection module to the ICAO PKD allowing the automation of exchanges: <ul style="list-style-type: none"> <li>• Systematic retrieval of all certificates already published by ICAO member Countries; and</li> <li>• Transmission of public keys, CRLs etc. to ICAO PKD.</li> </ul> This is in order to verify the authentication of documents at the border, in a flexible, user-friendly manner.
Req. 316.	Required	The eMRTD PKI system shall support the same algorithm on CSCA and the "Document signers" (DS) and shall support the cryptographic algorithms and key lengths recommended by the ICAO.
Req. 317.	Required	The Service Provider will ensure the transition from the CSCA already in place to the new solution, in compliance with ICAO standards "Guidance Document Migrating Country Signing Certification Authority (CSCA)" of April 2018.
Req. 318.	Required	The PKI solution shall implement the fingerprint protection mechanism in accordance with the "Extended Access Control" standard specified by BSI TR-3110. It shall manage the lifecycle of the keys and certificates of the Country Verifying Certification Authority (CVCA) which supports the issuance of Extended Access Control (EAC) in passport documents, allowing IS capabilities.

Reference	Required / Optional	Description of Technical requirements
Req. 319.	Required	The Service provider should operate this solution for quality control and if needed expand the operation to support other use cases over the country.
		<b>On-site queuing management solution</b>
Req. 320.	Required	Each enrolment site in Armenia operated by the Service provider shall have a queuing system with the objective to optimize the citizen flow for enrolment and issuance of ID documents.
Req. 321.	Required	The solution shall consider each specific configuration of enrolment sites (number of active enrolment station) in order to optimize the citizen flow according to the SLA.
Req. 322.	Required	Citizen should be informed upfront about expected waiting time.
Req. 323.	Required	The solution shall include a monitoring functionality that enables to follow the flow in one Service point as well as globally in all Service points of the country in real time.
		<b>Reports and statistics solution</b>
Req. 324.	Required	The solution shall include an analysis and reporting module that uses technical and functional logs to produce administration and operational reports (number of people enrolled, deduplication statistics, etc.).
Req. 325.	Required	The analysis and reporting module shall integrate a set of standard reports and shall allow reports to be customized according to the needs of the Authorities.
Req. 326.	Required	The analysis and reporting module shall at least integrate the following reports: <ul style="list-style-type: none"> <li>• Document blank production / stock management</li> <li>• Biometric documents produced</li> <li>• Defective documents</li> <li>• Distributed biometric documents to their holder</li> <li>• Documents waiting to be retrieved</li> <li>• Reports based on enrolment station, employee</li> <li>• Reports including statistics in order to follow the SLA,</li> <li>• Other aligned the design of reporting procedure defined in the chapter 2.6.2.</li> </ul>
		<b>Integrations with external data sources</b>
Req. 327.	Required	Service Provider shall implement and O&M IDMIS integration interfaces with external data sources necessary in the scope of operations in this Project (list is indicative and shall be aligned with the Contracting Authority during the design phase): <ul style="list-style-type: none"> <li>• Government Gateway – for user authentication and eSignature for eServices on Citizen eService application. Also, eServices on</li> </ul>

Reference	Required / Optional	Description of Technical requirements
		<p>Citizen eService application shall be accessible from Government Gateway.</p> <ul style="list-style-type: none"> <li>• Population registry – for identity validation during enrolment.</li> <li>• Legacy biometric data and document registry (current) - for biometric data matching / identity validation during enrolment (optional, if Service Provider chooses to migrate data from legacy biometric data and document registry to new one).</li> <li>• GoA appointed CA – for certificate integration during the personalization process, ID card/certificate lifecycle events (revocation/suspension).</li> <li>• Treasury ERP solution – for accounting reconciliation with GoA treasury on fees paid for document issuance.</li> <li>• MS ERP solution – for reporting and billing purposes (in case such solution shall be implemented by GoA).</li> <li>• Border guard IS - interface to provide data from Biometric data and document registry according to the national law requirements.</li> <li>• Other IS / Registries identified during the design phase.</li> </ul>

## 2.5. Service level agreement KPIs

**Note:** All requirements listed in this section below are required. However, please note that the Service providers who may suggest improved Service Level Agreements as part of their Technical Proposal shall be evaluated favorably as per methodology described in the Request for Proposal document.

Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
Req. 328.	<p>Enrolment facilities outside Yerevan shall be open Monday – Friday from 9:00 to 18:00 with no lunch break.</p> <p>At least one (1) facility in Yerevan shall be open Monday – Sunday from 9:00 to 18:00 with no lunch break.</p> <p>Other enrolment facilities in Yerevan shall be open Monday – Saturday from 9:00 to 18:00 with no lunch break.</p> <p>In all cases, open hours exclude public holidays in Armenia.</p>	<p>The Closed time is measured when a facility is closed during normal office hours. Closed time is not counted in the event of force majeure event (natural disaster, insecurity, etc.) or in the event the closed time has been previously agreed by the Contracting Authority for specific reason (e.g., election day, adjustment to actual demand, incident investigation, etc.).</p> <p>In the event a facility opens outside of normal office hours, then the extra time outside opening hours is accounted negatively in the Closed time.</p>	<p>Cumulative closed time within the official opening hours: &gt; 4,5 hours in a given facility</p>	<p>Cumulative closed time within the official opening hours: &gt; 18 hours in a given facility</p>	<p>&gt; 30% of facility network closed for more than 18 hours (cumulative closed time within the official opening hours in a given facility)</p>
Req. 329.	<p>The time between the application completion and the first available timeslot for a face-to-face appointment through the Citizen</p>	<p>Evidence based on data from Citizen web-application portal, Application Performance</p>	<p>&lt; 5 % of registration attempts</p>	<p>1. 5-20% of registration attempts</p>	<p>&gt;20 % of registration attempts</p>

Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
	<p>web-application portal shall be not more than:</p> <ul style="list-style-type: none"> <li>14 days for an ordinary request with 50 % of users being able to register for an appointment in 1 week</li> <li>1 day for a fast-track request</li> <li><b>Fast-track SLA does not apply to appointments outside Armenia (foreign missions) and MFA facilities in Yerevan.</b></li> </ul>	<p>Monitoring Tool or equivalent reliable data source must be provided, containing the following data:</p> <ul style="list-style-type: none"> <li>Timestamp of each application completion</li> <li>Timestamp of first available timeslot in user selected/preferred enrolment facility at the given moment of application completion</li> <li>Timestamp of first available timeslot in any enrolment facility at the given moment of application completion</li> <li>The percentage of users able to register for an appointment: (1) in 14 days for ordinary request, (2) in 1 week for ordinary request, (3) 1 day for a fast-track request (cumulative for all enrolment facilities in Armenia, excluding MFA facilities in Yerevan)</li> <li>Breach only exists if estimated quarterly volume of applications indicated in "Annex No. 3: Estimated services' volumes is not exceeded (estimated yearly capacity is divided by 4).</li> </ul>	exceed target	<p>exceed target</p> <p>OR</p> <p>2. If online registration system is not available or does not allow to register for more than 72 hours</p>	<p>exceed target</p> <p>OR</p> <p>If online registration system is not available or does not allow to register &gt;168 hours</p>
Req. 330.	Queue waiting time shall be no longer than 15 min for on-line registered applicants (turnaround time) in each enrolment facility	<p>Evidence based on data from queue management solution or equivalent reliable data source must be provided, containing the following data:</p> <ul style="list-style-type: none"> <li>Timestamp when each registered applicant enters the queue</li> <li>Timestamp when they start being served</li> <li>Turnaround (the waiting time in minutes for each applicant)</li> <li>Average turnaround time for each enrolment facility separately</li> </ul>	> 5% of cases exceed target waiting time across all facilities together	> 10% of cases exceed target waiting time across all facilities together	-



Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
		Note: the applicants who are not present at the appointment time allocated at the web-enrolment step are excluded from the calculation methodology.			
Req. 331.	Non-registered applicants' waiting time is managed through the queuing system. Queue waiting time shall be no longer than 2 hours for non-registered applicants (average turnaround time for all stations and enrolment facilities combined).	Evidence based on data from queue management solution or equivalent reliable data source must be provided, containing the following data: <ul style="list-style-type: none"> <li>• Timestamp when each non-registered applicant enters the queue</li> <li>• Timestamp when they start being served</li> <li>• Turnaround (the waiting time in minutes for each applicant)</li> <li>• Average turnaround time for each enrolment facility separately</li> <li>• Average turnaround time for all enrolment facilities combined</li> <li>• The percentage of applicants served within 2 hours (1) for each enrolment facility separately and (2) all facilities combined</li> </ul>	NA (only monitored)	NA (only monitored)	-
Req. 332.	An applicant shall spend maximum: <ul style="list-style-type: none"> <li>• 20 minutes during the enrolment process;</li> <li>• 15 minutes during the issuance process.</li> </ul>	Evidence based on data Identity management and document issuance solution or equivalent reliable data source must be provided, containing the following data elements: <ul style="list-style-type: none"> <li>• Timestamp when each applicant starts being served</li> <li>• Timestamp when each applicant finish being served (service is also deemed to be finished if enrolment process cannot be finalized for</li> </ul>	> 10 % of cases exceed target service time across all facilities together	-	-

Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
		<p>reasons the citizen is responsible for, e.g. non-availability of all necessary documents. Service is finished when enrolment is finalized; payment process is not included)</p> <ul style="list-style-type: none"> <li>• Turnaround (the serving time in minutes for each applicant)</li> <li>• Average turnaround time for each enrolment facility separately</li> <li>• Average turnaround time for all enrolment facilities combined for (1) enrolment process and (2) issuance process</li> <li>• The percentage of applicants served within: (1) 20 min for enrolment process and (2) 15 min for the issuance process for (1) for each enrolment facility separately and (2) all facilities combined</li> </ul>			
Req. 333.	<p><b>In Nominal mode (Ordinary request)</b></p> <p>The maximum time between the time when application/enrolment and vetting is completed (and successfully) and the time when document is ready to be issued in the service station shall be not more than 15 working days with 50 % of cases fulfilled within 10 working days after successful enrolment and vetting.</p>	<p>Evidence based on data from Identity management and document issuance solution or equivalent reliable data source must be provided, containing the following data elements:</p> <ul style="list-style-type: none"> <li>• Timestamp when application is submitted / enrolment is successfully completed (by Service Provider)</li> <li>• Timestamp when vetting is successfully completed (by Contracting Authority)</li> <li>• Timestamp when document is delivered to service station and is ready to be issued</li> <li>• Total turnaround time for every case</li> <li>• Average turnaround time for each enrolment facility separately</li> <li>• The percentage of cases completed within: (1) 10 working days and (2) 15 working days for (1)</li> </ul>	> 0,1 % of cases exceeding target service delivery time	0,5 - 5 % of cases exceeding target service delivery time	> 5 % of cases exceeding target service delivery time

Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
		for each enrolment facility separately and (2) all facilities combined			
Req. 334.	<p><b>In Fast-Track</b></p> <p>The maximum time between the time when application/enrolment and vetting is completed (and successfully) and the time when document is ready to be issued in the service station shall be:</p> <ul style="list-style-type: none"> <li>• Not more than 24 hours (excluding Sundays and public holidays), in case of document pick up in enrolment centers in Yerevan;</li> <li>• Not more than 48 hours (excluding Sundays and public holidays), in case of document pick up in enrolment centers outside Yerevan</li> <li>• Fast-rack SLA does not apply to applications outside Armenia (foreign missions) and MFA facilities in Yerevan.</li> </ul>	<p>Evidence based on data from Identity management and document issuance solution or equivalent reliable data source must be provided, containing the following data elements:</p> <ul style="list-style-type: none"> <li>• Timestamp when application is submitted and enrolment is successfully completed (by Service Provider)</li> <li>• Timestamp when vetting is successfully completed (by Contracting Authority)</li> <li>• Timestamp when document is delivered to service station and is ready to be issued</li> <li>• Total turnaround time for every case</li> <li>• Average turnaround time for each enrolment facility separately</li> <li>• The percentage of cases completed within: (1) 24 hours and (2) 48 hours for each enrolment facility separately and (2) all facilities combined</li> </ul>	> 0,1% of cases exceeding target service delivery time	0,5 – 5% of cases exceeding target service delivery time	> 5% of cases exceeding target service delivery time
Req. 335.	Minimum stock of blank documents shall meet the estimated demand for one year for every type of the blank document	<p>Evidence based on inventory count results or equivalent reliable data source.</p> <p>Demand estimated as per Annex No. 3: “Estimated services’ volumes”.</p>	-	Non-compliance result in Breach 2	-

Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
	at inventory dates 1 <sup>st</sup> January and 1 <sup>st</sup> July as of 2 <sup>nd</sup> operational year.				
Req. 336.	The citizen web portal shall be able to fully process 80 % of requests below 2 seconds.	Evidence based on Citizen web-application portal, Application Performance Monitoring Tool or equivalent reliable data source.  Breach only exists if estimated quarterly volume of applications indicated in “Annex No. 3: Estimated services’ volumes” is not exceeded (estimated yearly capacity is divided by 4).	> 10% of attempts exceed target waiting time	-	-
Req. 337.	100 % adherence to the customer service standard (prepared by the Service provider and verified by the Contracting Authority), verified by the independent mystery shopper or equivalent assessment, carried on the period basis (not less than once a year)	Mystery shopper or equivalent assessment, carried out on yearly basis by the independent third party selected jointly with the Contracting Authority at the expenses of the Service provider.	Non-compliance result in Breach 3	-	-
Req. 338.	For customer complaints and inquiries: <ul style="list-style-type: none"> <li>• Reaction time: 1 business day</li> <li>• Time to resolution: 10 business days, with 80 % of cases resolved in 5 business days</li> </ul>	Evidence based on customer complain and inquiries registering (help desk/ticketing) system logs or equivalent reliable data source.	10 - 30% of cases exceed target service delivery times	> 30% of cases exceed target service delivery times	-

Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
Req. 339.	The following provisions (applicable for hardware, software and equipment after handover) for reaction and resolution time for issues documented in the chapter “2.6.3 Hand back requirements”, “Requirements for warranty service”, “Requirements for maintenance and support services”.	Evidence based on help desk/ticketing system logs or equivalent reliable data source.	Any deviation of reaction and (or) resolution targets for critical mistakes	1. > 30% of cases exceed target service delivery times  OR  2. Deviation from resolution targets for critical mistakes > 72 hours	-
Req. 340.	Availability requirements for the Government and Public-Facing services (e.g.: enrolment services, issuance services, Citizen portal, the Migration Service and border control interface): <ul style="list-style-type: none"> <li>On a yearly basis at least 99% percent availability shall be guaranteed (a maximum of 87,6 hours of total downtime)</li> </ul>	Evidence based on data from performance monitoring tools, system logs analysis by each solution component, disaster recovery tests or other equivalent reliable data source.	NA (only monitored)	NA (only monitored)	NA (only monitored)

Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
	<ul style="list-style-type: none"> <li>RTO (Recovery time objective) – 14,4 min</li> <li>RPO (Recovery point objective) – 1 day</li> </ul> <p>Final list of services and related applications to be considered as Government and Public-Facing, will have to be aligned during the inception phase based on the solution architecture deployed by the Service provider.</p>				
Req. 341.	0 % of successful unauthorized access attempts on confidential data.	<p>Evidence based on data from system monitoring tools, system logs analysis by each solution component, or other equivalent reliable data source.</p> <p>Breaches are counted on hardware and software which is operated and maintained by Service Provider during contract period (i.e., not during warranty after hand back).</p>	Breaches not affecting sensitive personal data		Breaches affecting sensitive personal data
Req. 342.	The Service Provider shall inform the Contracting Authority about confidential data security breach within 4 hours of becoming aware of the breach.	NA	Deviation from target reaction time < 1 hour	Deviation from target reaction time for 1 – 4 hours	Deviation from reaction time > 4 hours
Req. 343.	The Service Provider shall provide SLA KPIs completion	NA	-	-	-

Reference	Description of Technical requirements	Calculation method and (or) evidence	Breach 3 (minor)	Breach 2 (medium)	Breach 1(critical)
	reports on quarterly basis unless agreed otherwise with the Contracting Authority. The Service Provider must present both raw data to calculate the KPIs as well as a KPI report.				
Req. 344.	For avoidance of doubt, calculation of SLAs excludes any downtime and/or any time spent by the Contracting Authority teams (based on the Table 4 - Roles and responsibilities of the Contracting Authority) to perform necessary actions or interventions within their operational scope and technical perimeter.	-	-	-	-

## 2.6. Requirements for the requested services

The Service Provider shall provide managed services of all solutions described above. Minimum requirements for services are provided below.

### 2.6.1. Design and implementation requirements

Reference	Description of Technical requirements
	<b>General requirements</b>
Req. 345.	<p>Operational phase of the project must start not later than 15 months from the date of Contract signing date.</p> <p>Full implementation of all requirements, incl. certification related requirements, set out in this document shall not exceed 24 months from the date of Contract signing date (Execution date).</p> <p>Gradual implementation of full obligations set the in Technical Requirements may be acceptable, e.g.:</p> <ol style="list-style-type: none"> <li>1. ID cards may start to be issued earlier than biometric passports</li> <li>2. Personalization facility with new IT infrastructure may become operational earlier than full scope redesign of enrolment facilities network</li> <li>3. Enrolment facilities can be rolled out in the phased approached</li> <li>4. Conformity assessment to relevant standards (e.g., PCI CPP, ISO 27001) must be completed prior the start of operations, but relevant certification (e.g., eIDAS) may be completed in later stages but no later than 24 months after the Execution date.</li> </ol> <p>Final implementation timeline shall be aligned with the Contracting Authority during the initiation phase in accordance with implementation plan proposed in the Technical Proposal of the Service Provider.</p>
	<b>Initiation phase</b>
Req. 346.	<p>In one (1) month after the commencement of the contract, The Service Provider shall provide the detailed plan containing a timetable, activities, milestones, and deliverables in alignment with their initial proposal, considering:</p> <ul style="list-style-type: none"> <li>• Time to complete design phase of the project</li> <li>• Time necessary to start issuing documents according to the requirements set in the chapter “2.3. Requirements for Travel and Identity documents”</li> <li>• Time necessary for reconstruction of enrolment facilities, roll out plan</li> <li>• Time necessary for reconstruction of personalization facility, roll out plan</li> <li>• Time necessary to launch and deliver all software, hardware, and equipment components necessary for end-to-end service delivery</li> <li>• Time necessary to hire and train employees</li> <li>• Supplier’s expectations regarding the Contracting Authority, in terms of decision making, consultations, desired expertise, manpower and facilities.</li> <li>• Other aspects, necessary for successful launch of operations</li> </ul>
Req. 347.	<p>During the initiation phase Service Provider shall align the implementation and roll-out plan with the Contracting Authority.</p>
	<b>Design phase</b>



Reference	Description of Technical requirements
Req. 348.	Service provider shall detail and align with the Contracting authority specifications of all the software, hardware, and equipment components necessary for end-to-end service in accordance with their initial technical proposal in bidding stage.
Req. 349.	Service provider shall provide and work together with the Contracting Authority to align the aesthetic design and physical security measures specification of documents.
Req. 350.	<p>Service provider shall detail and align with the Contracting authority a final detailed design of geographical network of enrolment facilities in alignment with their initial technical proposal in bidding stage, incl.:</p> <ul style="list-style-type: none"> <li>• Location</li> <li>• Form of ownership</li> <li>• Planned date of start of operations</li> <li>• Number of workstations</li> <li>• Interior and exterior design concept and specification</li> </ul>
Req. 351.	Service provider shall detail and align with the Contracting authority a final physical and logical structure design of personalization facility, data center and disaster recovery site.
Req. 352.	<p>Service provider shall provide and align with the Contracting authority a description of document issuance services, all the processes and relevant procedures, required human resources, IT systems and document forms including, but not limited to the following processes (<b>Process manual and operating procedures</b>):</p> <ul style="list-style-type: none"> <li>• Application and enrolment</li> <li>• Approval of applications and personalization order formation</li> <li>• Personalization</li> <li>• Quality control</li> <li>• Transportation of documents</li> <li>• Issuance to costumers</li> <li>• Post-issuance services</li> <li>• Vetting service (performed by the GoA employees)</li> </ul>
Req. 353.	Service provider shall provide and align with Contracting Authority a description of Contract reporting and compliance plan/procedures drafted in accordance with the requirements set in the Contract.
Req. 354.	Service provider shall provide and align with Contracting Authority clear data flow diagrams, architecture and security control and documentation (“checklist” and exception list).
	<b>Build and Test phase</b>
Req. 355.	The setup of a test program is the responsibility of the Service Provider; however, the Contracting Authority can ask an external competent party for a second opinion or contra expertise on the by the Service Provider executed tests.
Req. 356.	The Service Provider shall setup for all the different parts of the assignment a test and acceptance plan (test program). This plan shall be aligned with the Contracting Authority.
Req. 357.	<p>The Service Providers test and acceptance plan shall contain description of:</p> <ul style="list-style-type: none"> <li>• Test strategy</li> </ul>

Reference	Description of Technical requirements
	<ul style="list-style-type: none"> <li>• Test specifications</li> <li>• Test scenarios</li> <li>• Test environment</li> <li>• Procedures</li> <li>• Task and responsibilities</li> <li>• Execution plan / schedule</li> </ul>
Req. 358.	Any citizen facing portal or web product should include pre-launch testing with target users to identify any user experience improvements and ensure a smooth user journey. Test approach and test report shall be aligned with the Contracting Authority.
Req. 359.	Citizen facing web portals should meet WCAG 2.1 standards for accessibility, and user testing (see requirement above) shall include users with disabilities, to be defined with the Contracting Authority.
Req. 360.	Citizen facing web portals design should adopt service design principles and user interface graphics approved and in use by GoA during the duration of the Contract.
	<b>Project progress monitoring</b>
Req. 361.	The Service Provider will submit a written report once a week indicating in any case: <ul style="list-style-type: none"> <li>• What work has been done,</li> <li>• What progress has been made in relation to the project timetable,</li> <li>• Any problems/risks and the proposed solutions.</li> </ul>
Req. 362.	The Service Provider shall participate in regular Project progress meetings and prepare meeting minutes documenting the main issues discussed, agreed actions and decisions taken as well as deadlines for their completion.

## 2.6.2. End-to-end service operations' requirements

Reference	Description of Technical requirements
	<b>General</b>
Req. 363.	Providing all the personnel needed at the personalization facilities and the personnel handling the applications and issuing the documents (in enrolment facilities in the territory of Armenia) is part of the assignment. The Service Provider provides all their necessary training for all the personnel.
Req. 364.	All selected personnel will need to pass a background check by GoA.
Req. 365.	At the personalization site at any given time shall be a one officer responsible for the verification of the identity and authorization of people entering to facilities. Providing these officers is, as mentioned above, part of the assignment.
Req. 366.	The Service Provider shall implement and maintain a Security Program for the entire duration of the Agreement that incorporates appropriate administrative, technical, and physical security measures; ensures confidentiality, integrity, availability and security

Reference	Description of Technical requirements
	of the service's information, its users, and its systems, and which complies with eIDAS and ISO 27001.
Req. 367.	Service provider shall actively participate in the GoA working group capable of monitoring technological developments and safety and proactively provide recommendations for improvement of the security features of Identity and travel documents.
Req. 368.	Service Provider shall consult Contracting Authority regarding GoA process efficiency improvement and / or new functions (e.g., vetting process efficiency improvement, participation in ICAO organization).
Req. 369.	<p>Service provider shall prepare and align with Contracting Authority Contract monitoring and reporting procedures, KPIs and templates.</p> <p>Reporting shall include, but not limited to:</p> <ul style="list-style-type: none"> <li>• Financial information for billing purposes;</li> <li>• Document stock information;</li> <li>• SLAs performance;</li> <li>• Document quality issues in different stages (personalization, at issuance station prior issuance to customers, post document issuance to customers);</li> <li>• Maintenance works;</li> <li>• Updates and improvements implemented across all areas of the Contract;</li> <li>• Other agreed areas.</li> </ul>
	<b>Enrolment and related citizen facing services</b>
Req. 370.	Service provider must prepare customer service standard, train employees accordingly and ensure compliance to the standard during the Contract duration.
Req. 371.	<p>Service provider shall provide continued operations of the enrolment service in territory of Armenia, incl. but not limited to:</p> <ul style="list-style-type: none"> <li>• Receiving and fulfilling applications for travel and identity documents (first time, renewal, damaged, stolen, or lost documents, etc.);</li> <li>• Issuing the travel and identity documents in the customer enrolment stations;</li> <li>• Acting as registration authority for qualified eSignature according to eIDAS requirements;</li> <li>• Customer support services, incl. online/live support related to physical documents (e.g., in the case of lost/damaged document, other relevant issues);</li> <li>• Customer support services, online/live support for eID users (e.g., consultations, answers to requests, issuance of ID card readers, PIN code changes, etc.);</li> <li>• The post issuance services, incl. collection and destruction of expired or cancelled documents.</li> </ul> <p>These services must be provided without additional fees to customers (other than quoted in the financial proposal).</p>
Req. 372.	Enrolment operations shall be carried in compliance to ISO27001, ISO 9001 and, where applicable, eIDAS standards. Certificate of compliance is requested and proven by annual audits from an external accredited company.

Reference	Description of Technical requirements
Req. 373.	<p>Customer support services must be available on-site/ via email/ via phone/ via online system (e.g., tickets for obtaining post issuance services are possible to be submitted online).</p> <p>All customer complaints or requests must be registered in help desk/ticketing system, that would allow to log and track:</p> <ul style="list-style-type: none"> <li>• Time and date of the complaint or request</li> <li>• Reaction time</li> <li>• Resolution time</li> <li>• Accompanying documents of communication</li> </ul> <p>System logs must be accessible for the Contracting Authority for quality monitoring purposes.</p>
Req. 374.	Service provider must provide ordinary document issuance services, compliant to SLAs requirements described in the chapter 2.5. "Service level agreement KPIs".
Req. 375.	Service provider must provide fast-track document issuance services, compliant to or exceeding SLAs requirements described in the chapter 2.5. "Service level agreement KPIs".
Req. 376.	Service provider must propose service delivery model, align it with GoA and provide free of charge enrolment service for citizens with limited mobility (e.g., in hospitals).
Req. 377.	When documents are issued (securely delivered) in the enrolment facilities, these services must be provided without additional fees to customers (other than regulated tariff).
Req. 378.	Documents can be issued (securely delivered) by other means / in other locations than enrolment facilities, subject it is compliant with local laws, regulations and standards specified in this document. These services may be provided with additional fees to customers defined by the Service provider.
Req. 379.	Service provider shall provide free of charge for citizens various certificates / notices related to the status of their travel and identity documents. Document forms and types shall be aligned with Contracting Authority during the design phase of the Project.
Req. 380.	Service provider shall request physical face to face presence of the citizen at least once during the overall process from enrolment to issuance (secure delivery).
Req. 381.	Service provider must maintain content of the informational web portal (specified in the section "Requirements for the Identity and Document Management System") providing up to date user friendly information to citizens about fees and procedures related to customer services provided in the scope of this Tender.
Req. 382.	Service provider must prepare and align with the Contracting Authority "the book of document quality", defining document quality parameters.
Req. 383.	Service provider must act as a primary contact point in case of customer complaints free of charge for customer. Should Service provider be not able to solve the dispute with the customer, Service provider must escalate the dispute to the Contract Authority for final resolution.
Req. 384.	Issued documents shall be warranted by the Service provider. Should customer complain regarding document quality be proven to be justified (document does not

Reference	Description of Technical requirements
	meet criteria listed in “the book of document quality”), customer shall be issued a new document as a fast-track service (in 1 day, excluding Sundays and public holidays) free of charge.
	<b>Personalization service</b>
Req. 385.	<p>Service provider shall provide continued document personalization, incl. but not limited to:</p> <ul style="list-style-type: none"> <li>• Document blank supply and management</li> <li>• Document personalization</li> <li>• Provide production follow up services, incl. quality control, stock management, traceability and tracking of the produced documents</li> <li>• Logistical operations and transport from document blank production location to personalization facility</li> <li>• Logistical operations and transport of personalized documents from personalization facility to enrolment facilities in the territory of Armenia</li> <li>• Note: logistical operations and transport from personalization facility to enrolment facilities outside Armenia will be handled by GoA, but Service Provider is responsible for secure hand over of personalized documents to GoA for further transportation.</li> </ul>
Req. 386.	Personalization operations shall be carried in compliance to ISO 27001, ISO 9001 and PCI CPP standards. Certificate of compliance and applicability issued by the competent body shall be made available upon request.
Req. 387.	The Service Provider shall implement a waste control system for the personalization process, in compliance with Health Regulation or the regulation that is in force in GoA. The Service Provider shall be responsible for the removal and handling of all waste produced during the personalization process.
Req. 388.	Defective blank and personalized documents shall be treated as waste and destroyed with adapted shredders regarding sensitivity of the documents. Their destruction must be logged: all blanks entering the facility must either exit as waste or as personalized documents.
Req. 389.	The Service Provider shall provide all supplies needed to personalize the documents. Service provider shall ensure security of document blanks during the transportation and handling.
Req. 390.	The GoA will classify the personalization site as “special importance facility” and will ensure external guarding by the Armenian police during 24 hours a day free of charge.
Req. 391.	The Service Provider shall take all necessary measures and precautions to prevent, detect, diminish and/or control risks and threats regarding disturbance of the personalization process, demolition of the infrastructure, equipment and data, theft, and forgery and other possible security events.
Req. 392.	The Service provider shall provide production follow up services, incl. quality control, stock management, traceability and tracking of the produced documents.
Req. 393.	The Service Provider shall transport personalized documents from the personalization site to the application and issuing locations throughout Armenia.

Reference	Description of Technical requirements
Req. 394.	Transportation takes place in a controlled and secure way that minimalizes the risk of theft, robbery, loss or destruction of documents, the risk of unlawfully behavior of personnel of the transport company and the risk of delays.
Req. 395.	PIN mailers shall not be transported in the same transport as the personalized document. PIN mailers of a document shall be transported with the next transport (after the transport of the personalized document).
Req. 396.	The transportation of personalized documents shall be carried out using trusted logistics, ensuring monitoring and traceability of the process. Controlled procedure of the chain of custody has to be implemented.
Req. 397.	Service Provider shall ensure that all the blank documents, semi-finished products and security materials needed to personalize are timely available at the personalization site and are transported in a controlled and secure way that minimalizes the risk of theft, robbery, loss or destruction of documents, the risk of unlawfully behavior of personnel of the transport company and the risk of delays.
Req. 398.	The Service Provider shall ensure stock of document blanks stored in Armenia to meet average expected document demand for 1 year for all duration of the Contract.
	<b>Maintenance of software, hardware, and equipment, incl. technological infrastructure</b>
Req. 399.	<p>Service provider shall provide maintenance and operations of global IT system (software, hardware, and equipment) for the contract duration, for the infrastructure deployed in territory in Armenia and in enrolment stations in foreign missions, incl. but not limited to the following global IT system components:</p> <ul style="list-style-type: none"> <li>• Technological infrastructure, as defined in chapter “2.2.3. Requirements for technological infrastructure”</li> <li>• Identity and Document Management Information System, as defined in chapter “2.4. Requirements for Identity and Document Management Information System”</li> </ul>
	<b>Maintenance of the physical facilities of enrolment and personalization</b>
Req. 400.	<p>Service provider shall provide maintenance and operations of all the physical facilities operated by the Service provider in the territory of Armenia (as defined in chapters “2.2. Requirements for physical infrastructure”) in scope of this Contract for the Contract duration, including, but not limited to:</p> <ul style="list-style-type: none"> <li>• Maintenance of the physical condition of facilities.</li> <li>• Cleaning service.</li> </ul>
	<b>Additional Services or infrastructure related to the object of the Contract</b>
Req. 401.	Service provider shall provide up to 1 000 additional hours of services related to improvements and needs of IDMIS technical or functional requirements identified by the Contracting Authority and (or) the Service Provider.

### 2.6.3. Hand back requirements

Reference	Description of Technical requirements
Req. 402.	<p>Service Provider must transfer all assets back to the Contacting Authority (please refer for the detailed procedure in the Contract):</p> <ul style="list-style-type: none"> <li>• Registry – after the implementation phase is completed and Registry is accepted.</li> <li>• Assets implemented in the premises of MFA – after the implementation phase is completed and assets are accepted.</li> <li>• The rest of assets – at the end of the Contract.</li> </ul>
Req. 403.	All assets handed back to the Contacting Authority must meet minimum requirements, specified in the “Annex No. 5: Minimum Requirements for Asset Hand back”.
Req. 404.	<p>The Registry and assets implemented in the premises of MFA (all assets that will be implemented in the scope of the Contract but will not be operated by the Service provider) shall be warranted until the end of the Contract.</p> <p>The rest of assets (what will be operated by the Service provider for the duration of the Contract) shall be warranted 1 year after the hand back is completed. Warranty requirements are specified in this chapter below.</p>
Req. 405.	Service provider must train not less than 100 GoA appointed employees according to requirements specified in this chapter below in the scope of hand back procedure.
Req. 406.	Travel and identity documents according to requirements set in this document must continue to be issued to citizens until the hand back is successfully completed.
Req. 407.	Hand back must include stock of blank documents for 1 year of estimated demand.
Req. 408.	<p>Before hand back is completed, Service Provider must transfer the following documentation for the Contracting Authority:</p> <ol style="list-style-type: none"> <li>1. Technical specification of all assets, incl.: <ul style="list-style-type: none"> <li>• Description of logical architecture.</li> <li>• Description of the realization of the requirements set in this document, providing references to specific software functions, user interface screens, applicable rules and limitations, other relevant information)</li> <li>• Description of IDMISS configuration parameters (rules, settings);</li> <li>• Description of data base structure and data model;</li> <li>• Description of reports and forms;</li> <li>• Description of integrations with external data sources, its’ management rules;</li> <li>• Description of additional (programmable / non-standard) functionality. The description of additional functionality should include, but not limited to description of the functionality program code in all levels of the architectural model; Source Codes and their functional logic diagrams;</li> <li>• Data flow diagrams, architecture and security control documentation (“checklist” as well as “exception lists”);</li> </ul> </li> </ol>

Reference	Description of Technical requirements
	<p>3. User and administrator manuals / instructions;</p> <p>4. User trainings materials (incl. guidelines in video format, where the full process of application and printing of passports will be shown including people (simulation or real process) with combination of IT solution procedures on the computer screen);</p> <p>5. Specification of user roles and rights configuration (incl. matrix of user role and associated rights);</p> <p>6. Technical infrastructure specification, incl. physical and logical architecture design description: physical components and preliminary need for their capabilities (CPU, RAM, disk space, IOPS); connections between components and required network access; Software implemented in the components (OS, DBMS, application servers and other software); location of components in different network areas with different accessibility.</p> <p>7. The disaster recovery plan;</p> <p>8. Customer service standard description;</p> <p>9. Descriptions of all processes and procedures, incl. instructions for all of operations in scope of the Contract, providing details on steps to be performed, IT systems to be used, documents/reports/forms to be generated and other relevant information;</p> <p>10. Job descriptions for all positions in scope of the Contract.</p>
	<p><b>Requirements for licensing conditions</b></p>
Req. 409.	The number of IDMISS internal and external users, administrators shall not be limited by licenses.
Req. 410.	IDMISS must be able to store unlimited data lines, without the need to acquire additional software licenses.
Req. 411.	The volume of data processed by IDMISS should not be limited by software licenses.
Req. 412.	Software licenses must not restrict future developments of the solution (by modifying existing or creating new functional components, reports, and other system components).
Req. 413.	<p>All software licenses must be perpetual and must have other necessary permissions for software usage, whether the technical maintenance and support services from the software manufacturer or Service provider have been purchased.</p> <p>If the manufacturer, according to its policy, does not provide perpetual licenses, the Service provider must provide official certificate from the manufacturer and other supporting evidence (e.g., the manufacturer's licensing policy).</p> <p>In this case, the software license must be valid for at least 10 years after hand back,</p>
Req. 414.	If the technical maintenance and support of the licenses is not purchased, the software should not stop working and should be fully functioning unlimitedly in time (or for a minimum of 10 years if the manufacturer's policy restricts the provision of an unlimited license), up to the last version of the software released, during the period of Contract duration.



Reference	Description of Technical requirements
Req. 415.	The Service provider must provide license technical maintenance services throughout the term of the Contract.
Req. 416.	IDMIS licenses must provide Contracting Authority with access to at least 3 system environments: PROD, TEST, and DEV.
	<b>Requirements for development, testing and production environments</b>
Req. 417.	<p>Service Provider shall deliver and hand back three fully independent environments, incl. all the required software and hardware. Required environments:</p> <ul style="list-style-type: none"> <li>• PROD - production environment; this is the environment with which the System users work.</li> <li>• DEV - development environment; this is the environment in which the system is programmed, changed.</li> <li>• TEST - a test environment is an environment, where a new (or updated) functionality is loaded for testing.</li> </ul>
Req. 418.	PROD and TEST environments should have same hardware and software configuration.
Req. 419.	<p>During the design and implementation phase:</p> <ul style="list-style-type: none"> <li>• DEV environment must operate in the Service Provider's data center.</li> <li>• TEST environment must operate in both Service Provider's data center and in the data center provided by the Contracting Authority with the possibility to transfer it to another data center without performing significant development works of system components.</li> <li>• PROD environment must operate in the Contracting Authority's data center with the possibility to move it to another data center without performing significant development works of system components).</li> </ul>
Req. 420.	After the hand back, the DEV, TEST and PROD environment must operate in the data center provided by the Contracting Authority with the possibility to move it to another data center without performing major system software changes / redevelopments.
Req. 421.	IDMIS shall have means to periodically update the data for the DEV and TEST environments from the PROD environment. All personal data from PROD environment shall be anonymized.
Req. 422.	Developed software must be compiled in the environment of the Contracting Authority from the source texts of the software, stored in the Contracting Authority's source repository (Git or equivalent). The requirement applies only to the part of the software that was programmed during the custom development, but the Contracting Authority does not require the Source Codes of the offered standard market products.
Req. 423.	All the non-standard programmable software Source Codes, all tools as well as configurations, which ensure the full installation of the software at Contracting Authority environment, will have to be transferred to the Contracting Authority.
Req. 424.	The installation of the databases must be carried out from the script, placed in the Contracting Authority's Source Code repository (Git or equivalent), by using installation control systems (e.g., FlywayDB or equivalent) and performing installations, applying automated means such as Jenkins or equivalent. Installation

Reference	Description of Technical requirements
	instructions shall be prepared and handed over to the Contracting Authority before the implementation phase.
	<b>Requirements for warranty service</b>
Req. 425.	Warranty service must start after the hand back is completed.
Req. 426.	<p>The conditions of the warranty service, i.e., maintenance without additional payment, must meet the following requirements:</p> <ul style="list-style-type: none"> <li>• The purpose of the warranty service is to correct any defect in the IDMIS, Chip, OS and ID card middleware (together here referred as System), incl. all software, hardware and equipment, according to the requirements of this document, and all documents drafted and delivered during the design, implementation, and operation (when applicable) phase;</li> <li>• Duration of warranty service: <ul style="list-style-type: none"> <li>○ The Registry and assets implemented in the premises of MFA (all assets that will be implemented in the scope of the Contract but will not be operated by the Service provider) shall be warranted until the end of the Contract.</li> <li>○ The rest of assets (what will be operated by the Service provider for the duration of the Contract) shall be warranted 1 year after full acceptance (hand back), counting from the date of the hand back.</li> </ul> </li> </ul>
Req. 427.	<p>Warranty service by the Service Provider must be performed in accordance with the agreed procedures. Service provider must design and align with the Contracting Authority the policy and procedures on warranty and maintenance services. The policy and procedures for the warranty and maintenance services must specify in detail the Service provider's responsibilities and tasks, terms and conditions for resolving errors, quality management plan, procedures for change, risk and problem management procedures and the optimal communication plan.</p> <p>Warranty policy and procedures must be prepared prior the start of the operations in the scope of the Contract.</p>
Req. 428.	<p>The different levels of support are classified:</p> <ul style="list-style-type: none"> <li>• <b><u>Level 1 Support (Contracting Authority)</u></b>: The responsibility of Level 1 Support is to register and classify Incidents and to undertake an immediate effort in order to restore a failed Hardware incident or IT Service as quickly as possible.  Level 1 Support processes Service Requests, keeps users informed about their incidents' status at agreed intervals, gives the elements requested by Level 2 Support.  Level 1 Support also undertakes the activities of Preventive Maintenance (hardware and software)</li> <li>• <b><u>Level 2 Support (Contracting Authority)</u></b>: Support takes over incidents which cannot be solved regarding the complexity with the means of Level 1 Support.  The aim is to perform curative maintenance (workaround) and then to fix the problem (corrective maintenance).</li> </ul>

Reference	Description of Technical requirements
	<p>Level 2 Support includes tests that should be performed either to investigate or to reproduce the problem or validate the solution after correction.</p> <p>If no solution can be found, the Level 2 Support contacts Level 3 Support of the Service Provider.</p> <ul style="list-style-type: none"> <li>• <b><u>The Level 3 Support (Service provider):</u></b> The responsibility of Level 3 Support is to register and classify requests generated by the L2 support. The L3 support is represented by experts in the premises of the Service provider and is responsible of bug analysis, investigation, and fixes. The Level 3 Support requires high level of expertise (high knowledge of Service provider or its licensors proprietary products, IT technologies, data base experts, etc.) and when necessary, the L3 Support uses specific tools such as remote connection to ensure a high level of reactivity.</li> </ul> <p>As a result, the L3 Support provides a solution (workaround, corrective patch, etc.) to be tested and applied locally by the Level 2 Support of the Contracting Authority.</p>
Req. 429.	<p>The warranty service of the System shall include a L3 support by the Service Provider for the following:</p> <ul style="list-style-type: none"> <li>• Remedy of non-compliance of the System to the requirements set in this document and elimination of errors;</li> <li>• Restoration of functioning of the operational System, e.g., in case of malfunctions of a database or its components, where it is caused by the updates provided by the Service Provider or other actions or non-action of the Service Provider. Non-action of the Service provider shall mean that Service Provider did not take any actions where malfunction of databases or their components is identified during the System operation, or, where the Service Provider fails to notify the Contracting Authority of the System updates provided to him by the manufacturer (which have or may have an impact on the proper functioning of the System);</li> <li>• Recovery of damaged (corrupted) data when the failure is caused by incorrect operation of the software provided by the Service Provider;</li> <li>• Consultations by phone and e-mail to the key users of the IDMIS (estimated approximate number of key users of the IDMIS shall be no less than 5);</li> <li>• Monitoring of technical vulnerabilities of the System software performed by the system manufacturer, notification of discovered vulnerabilities and provision of updated versions to repair vulnerability gaps;</li> <li>• Removal of problems and errors where the System does not work or is not functioning correctly not because of incorrect implementation of the functional requirement or operational logic, but because of other components of the solution provided by the Service Provider, e.g., functionality of the standard software. These problems include: the submitted standard functionality of the System negatively affects (data is incompletely or incorrectly stored) the results of functional requirements; the provided database management system negatively affects the results of functional requirements (e.g., IDMIS performance, etc.). The Service Provider is responsible only for his provided software, including standard and customized software, and for the software for which he has defined the requirements (e.g., if the Service Provider formulates the requirement that the seamless operation of the System requires at least a certain version of a browser</li> </ul>

Reference	Description of Technical requirements
	<p>or a database management system, the System must operate with this browser or the database management system, and in the event of problems the Service Provider will be responsible for resolving the errors);</p> <ul style="list-style-type: none"> <li>• Modification, editing, adding of up to 20 basic functions within a calendar month. A basic function means generating data extracts and their delivery on the screen, completion and submission of context help, layout of function keys on the screenshot etc.</li> <li>• Repair and Replacement of Hardware: The Service provider is responsible for repair and return of defective hardware components under an RMA (Return Material Authorization) process. Spare parts, owned by the Contracting Authority, may only be used to replace defective System components.</li> </ul>
Req. 430.	<p>The Contracting Authority can perform independent Penetration and Vulnerability testing. If errors and non-conformities with the requirements of the technical specification are identified during this testing, the Service Provider will provide L3 support for eliminating these errors.</p>
Req. 431.	<p>All errors and/or problems of the Registry are classified:</p> <ul style="list-style-type: none"> <li>• Critical error – the error and/or problem preventing the IDMIS user to perform the necessary functions and no other way of performing the function is known or acceptable to the Contracting Authority;</li> <li>• Medium error – the error and/or problem preventing to perform the necessary functions, however, an alternative way of performing the function and acceptable to the Contracting Authority is available;</li> <li>• Minor error – the error and/or problem that basically does not prevent the reforming of necessary functions, but causes difficulty/discomfort to use the IS.</li> </ul>
Req. 432.	<p>The decision on the type of error (Critical error, Medium error, Minor error) is made by the responsible persons appointed by the Contracting Authority, in alignment with the responsible persons assigned by the Service Provider. Response time during which the Service Provider is required to analyze the error and/or problem and submit a description of the remedy of errors and/or problems to the Contracting Authority:</p> <ul style="list-style-type: none"> <li>• For Critical errors – 1 working hours;</li> <li>• For Medium errors – 1 working -day;</li> <li>• For Minor errors – 3 working days.</li> </ul>
Req. 433.	<p>Error and/or troubleshooting deadlines are approved by the Contracting Authority but must not exceed (the term is calculated starting from the moment of notifying of the problem and/or error):</p> <ul style="list-style-type: none"> <li>• For Critical errors – 1 working day (unless agreed otherwise with the Contracting Authority);</li> <li>• For Medium errors – 3 working days (unless agreed otherwise with the Contracting Authority);</li> <li>• For Minor errors – 10 working days (unless agreed otherwise with the Contracting Authority).</li> </ul>

Reference	Description of Technical requirements
	Detailed warranty service procedures and rules of procedure will be agreed during the preparation of the regulation for the System warranty service and System user consultation.
Req. 434.	<p>The Service Provider must provide the incident management (ticketing) solution (give access) for the registration and management of problems identified during the warranty service. The incident management solution has to be available on the browser on the website and to require no installation in the computers of the Contracting Authority. All problems should be stored in one place, ensuring their availability, confidentiality, and security.</p> <p>Reports about remedied (corrected) errors and/or problems, their resolution time must be submitted once a month.</p>
Req. 435.	The Service Provider must have ISO27001 Information Security Management Systems (ISMS) Certification for providing the warranty services.
Req. 436.	<p>Where the System is modified during the course of the warranty service work, the results of changes (modifications) must be provided to the Contracting Authority and versions of changes of the System must be released in accordance with the procedure agreed with the Contracting Authority. The Service Provider has to evaluate which existing System documentation is affected by changes (modifications) and what documentation is required for the successful implementation of change and its subsequent use, and submit all relevant documents, including but not limited to:</p> <ul style="list-style-type: none"> <li>• Data model, description of data structures for changes of the database objects.</li> <li>• If the System is installed in parts, and if the functionality of part of the System has been changed – description of the affected part of the System technical specification.</li> <li>• User manual (affected part).</li> <li>• Computer-based information help (e.g., HTML Help, etc.) component for changes of the functionality of the IDMIS (or part of the IDMIS) related to the component.</li> <li>• Installation manual for changes of the installation procedures.</li> <li>• Data set management (transfer) rules and encoded data set management (transfer) software (e.g., Scripts) in case of changes of the data set management (transfer) software.</li> <li>• IDMIS administration manual where such manual had to be reviewed.</li> <li>• Installation description of the change version of the IDMIS (with the description of changes included in the version, or sequence of the version installation).</li> </ul> <p>The documentation should be updated in a cumulative way, i.e., single updated document is provided instead of a separate amendment document.</p>
Req. 437.	Service provider must provide monthly reports on the warranty services (errors and/or problems eliminated (corrected)).
	<b>Requirements for maintenance and support services</b>
Req. 438.	Service provider must ensure the support and maintenance of the hardware, software and equipment (System) operated by the Contracting Authority after the Contracting Authority approves the purchase order as per price specified in the Financial proposal.

Reference	Description of Technical requirements
	The support and maintenance service may be requested yearly starting after the handover period with a maximum of 3 possible renewals.
Req. 439.	The object of maintenance and support services is all software, hardware and equipment (System) defined in the requirements of this document, and all documents drafted and delivered during the design, implementation, and operation (when applicable) phase.
Req. 440.	<p>Maintenance and support services by the Service Provider must be performed in accordance with the agreed procedures. Service provider must design and align with the Contracting Authority the policy and procedures on maintenance and support services. The policy and procedures for the maintenance and support services must specify in detail the Service provider's responsibilities and tasks, terms and conditions for completing change requests, resolving errors, quality management plan, procedures for change, risk and problem management procedures and the optimal communication plan.</p> <p>Maintenance and support policy and procedures must be prepared prior the end of handover.</p>
Req. 441.	<p>The maintenance and support services service shall include:</p> <ul style="list-style-type: none"> <li>• Processing and implementation of change requests submitted by the Contracting Authority (up to 1 000 hours per year) for change request implementation (whereas the number of maintenance and support hours dedicated to addressing System vulnerabilities shall not be limited). These change requests may involve modifications to the functionality or interfaces that alter, but do not fundamentally redesign, the system's core architecture. Typical requests may include but is not limited to customization of reporting tools, updates to user interface and integrations with external information systems or registries, functionality improvement as per necessary legal changes or international best practices. Each change request will be assessed, and modifications will be implemented within a reasonable timeframe based on complexity and scope. The Service Provider will ensure that these changes are integrated seamlessly without disrupting system performance or core functionality.</li> </ul> <p>The Service provider shall provide L3 support (as per definition in Req. 428) for the following<sup>2</sup>:</p> <ul style="list-style-type: none"> <li>• Remedy of non-compliance of the System to the requirements set in this document and elimination of errors;</li> <li>• Restoration of functioning of the operational System, e.g., in case of malfunctions of a database or its components, where it is caused by the updates provided by the Service Provider or other actions or non-action of the Service Provider. Non-action of the Service provider shall mean that Service Provider did not take any actions where malfunction of databases or their components is identified during the System operation, or, where the Service Provider fails to notify the Contracting</li> </ul>

<sup>2</sup> Please note, the services listed below for the first 1 (one) year after handover must be provided free of charge as a warranty service, regardless of if maintenance and support service is purchased or not. Starting the second year after the handover, it shall be provided only if maintenance and support service are purchased.

Reference	Description of Technical requirements
	<p>Authority of the System updates provided to him by the manufacturer (which have or may have an impact on the proper functioning of the System);</p> <ul style="list-style-type: none"> <li>• Recovery of damaged (corrupted) data when the failure is caused by incorrect operation of the software provided by the Service Provider;</li> <li>• Consultations by phone and e-mail to the key users of the IDMIS (estimated approximate number of key users of the IDMIS shall be no less than 5);</li> <li>• Monitoring of technical vulnerabilities of the IDMIS software performed by the system manufacturer, notification of discovered vulnerabilities and provision of updated versions to repair vulnerability gaps;</li> <li>• Removal of problems and errors where the System does not work or is not functioning correctly not because of incorrect implementation of the functional requirement or operational logic, but because of other components of the solution provided by the Service Provider, e.g., functionality of the standard software. These problems include: the submitted standard functionality of the System negatively affects (data is incompletely or incorrectly stored) the results of functional requirements; the provided database management system negatively affects the results of functional requirements (e.g., IDMIS performance, etc.). The Service Provider is responsible only for his provided software, including standard and customized software, and for the software for which he has defined the requirements (e.g., if the Service Provider formulates the requirement that the seamless operation of the System requires at least a certain version of a browser or a database management system, the System must operate with this browser or the database management system, and in the event of problems the Service Provider will be responsible for resolving the errors).</li> <li>• Repair and Replacement of Hardware: The Service provider is responsible for repair and return of defective hardware components under an RMA (Return Material Authorization) process. Spare parts, owned by the Contracting Authority, may only be used to replace defective System components.</li> </ul>
Req. 442.	<p>The Contracting Authority can perform independent Penetration and Vulnerability testing. If errors and non-conformities with the requirements of the technical specification are identified during this testing, the Service Provider will provide L3 support for eliminating these errors.</p>
Req. 443.	<p>All errors and/or problems of the Registry are classified:</p> <ul style="list-style-type: none"> <li>• Critical error – the error and/or problem preventing the IDMIS user to perform the necessary functions and no other way of performing the function is known or acceptable to the Contracting Authority;</li> <li>• Medium error – the error and/or problem preventing to perform the necessary functions, however, an alternative way of performing the function and acceptable to the Contracting Authority is available;</li> <li>• Minor error – the error and/or problem that basically does not prevent the reforming of necessary functions, but causes difficulty/discomfort to use the IS.</li> </ul>
Req. 444.	<p>The decision on the type of error (Critical error, Medium error, Minor error) is made by the responsible persons appointed by the Contracting Authority, in alignment with the responsible persons assigned by the Service Provider. Response time during</p>

Reference	Description of Technical requirements
	<p>which the Service Provider is required to analyze the error and/or problem and submit a description of the remedy of errors and/or problems to the Contracting Authority:</p> <ul style="list-style-type: none"> <li>• For Critical errors – 1 working hour;</li> <li>• For Medium errors – 1 working day;</li> <li>• For Minor errors – 3 working day hours.</li> </ul>
Req. 445.	<p>Error and/or troubleshooting deadlines are approved by the Contracting Authority but must not exceed (the term is calculated starting from the moment of notifying of the problem and/or error):</p> <ul style="list-style-type: none"> <li>• For Critical errors – 1 working day (unless agreed otherwise with the Contracting Authority);</li> <li>• For Medium errors – 3 working days (unless agreed otherwise with the Contracting Authority);</li> <li>• For Minor errors – 10 working days (unless agreed otherwise with the Contracting Authority).</li> </ul> <p>Detailed maintenance and support service procedures and rules of procedure will be agreed during the preparation of the regulation for the System maintenance and support services and System user consultation.</p>
Req. 446.	<p>The Service Provider must provide the incident management (ticketing) solution (give access) for the registration and management of problems identified during the maintenance and support services. The incident management solution has to be available on the browser on the website and to require no installation in the computers of the Contracting Authority. All problems should be stored in one place, ensuring their availability, confidentiality, and security.</p> <p>Reports about remedied (corrected) errors and/or problems, their resolution time must be submitted once a month.</p>
Req. 447.	<p>The Service Provider must have ISO27001 Information Security Management Systems (ISMS) Certification for providing the maintenance and support services.</p>
Req. 448.	<p>Where the System is modified during the course of the maintenance and support service work, the results of changes (modifications) must be provided to the Contracting Authority and versions of changes of the System must be released in accordance with the procedure agreed with the Contracting Authority. The Service Provider has to evaluate which existing System documentation is affected by changes (modifications) and what documentation is required for the successful implementation of change and its subsequent use and submit all relevant documents.</p>
Req. 449.	<p>Service provider must provide:</p> <ul style="list-style-type: none"> <li>• Monthly reports on the maintenance and support services (errors and/or problems eliminated (corrected));</li> <li>• Routine Meetings: monthly online meetings to review incident status.</li> <li>• Maintenance Visit: and one annual maintenance visit in Armenia.</li> </ul>



Reference	Description of Technical requirements
<b>Requirements for trainings</b>	
Req. 450.	Perform trainings before the start of handover of IDMIS (or its separate components).
Req. 451.	Together with the Contracting Authority, the Service Provider will have to prepare and confirm the lists of participants and create training groups.
Req. 452.	The size of the training group instructed by the Service Provider cannot exceed 10 persons.
Req. 453.	The Service provider will have to conduct training and prepare training material in Armenian and English. Only training of the Administrator user group can be conducted in English, but translation into Armenian will have to be ensured, where necessary.
Req. 454.	The Service provider will not prevent the Contracting Authority from filming and photographing the training conducted by the Service Provider.
Req. 455.	The Service Provider will have to prepare and confirm with the Contracting Authority the training programme and the training material which shall consist of a set of training themes and practical tasks. No later than 3 (three) weeks before the start of the training (if the Contracting Authority proposes no other time limit) the Service provider will have to confirm the training programme with the Contracting Authority.
Req. 456.	The Service provider will have to ensure participant registration at the time of training. The registration shall record participant's name, surname and signature confirming participation in the programme (registration will have to take place on each training day).
Req. 457.	The Service provider will have to prepare and distribute training material to each training participant (training material in the electronic form).
Req. 458.	The Service provider will have to ensure that for each type of training, representatives of the Service Provider will be able to answer the training participants' questions related to actual operations of the IDMIS.
Req. 459.	The Service provider must develop an operational training environment (the version of the IDMIS used for training) that can be used even after the training has been completed.
Req. 460.	The Service provider must perform users' knowledge assessment. The task will be considered completed when the users' knowledge assessment report is developed and approved by Contracting Authority.
Req. 461.	<p><b>User group 'Users' training (train the trainer type)</b></p> <p>Purpose of the training – train the Contracting Authority employees to use IDMIS.</p> <p>Goals of the training:</p> <ul style="list-style-type: none"> <li>• Provide the knowledge on: <ul style="list-style-type: none"> <li>• IDMIS functioning principles and logic.</li> <li>• User and their access rights management (where applicable).</li> </ul> </li> </ul>

Reference	Description of Technical requirements
	<ul style="list-style-type: none"> <li>• management of IDMIS configurable parameters;</li> <li>• management of classifiers.</li> <li>• IDMIS functions and operations.</li> <li>• Train the training participants to properly use the and perform operations.</li> <li>• Provide solutions to the questions raised during the trainings.</li> </ul> <p>The Service Provider will have to:</p> <ul style="list-style-type: none"> <li>• Train at least 100 training participants;</li> <li>• Conduct trainings lasting at least 1 day (8 hours) per training participant.</li> </ul>
Req. 462.	<p><b>User group 'IT administrators' training</b></p> <p>Purpose of the training – train the employees, who will be technically able to maintain the appropriate functioning of the IDMIS and other software components in scope of handover.</p> <p>Service provider has / will have to:</p> <ul style="list-style-type: none"> <li>• Train at least 5 training participants;</li> <li>• Conduct trainings lasting at least 1 day (8 hours) per training participant.</li> </ul>

#### 2.6.4. Special provisions for design, implementation, and hand back of the Biometric data and document registry (Registry)

This chapter provides a description of special provisions on the design, implementation, and acceptance (hand back) process since the Registry will be handed over the Contracting Authority after successful implementation. Service provider will not operate the Registry.

Reference	Description of Technical requirements
<b>Procedure for document acceptance</b>	
Req. 463.	The duration of the alignment of deliverables depends on the scope of the document. The Contracting Authority submits comments within 3 working days if the document is up to 10 pages long. If the volume of the document is bigger, the Contracting Authority shall submit comments within 5-10 working days. A specific deadline for comments will be agreed for each document longer than 10 pages.
Req. 464.	The Service Provider takes the comments into account and submits an updated document within 3 working days if the document is up to 10 pages long. If the volume of the document is larger, the Service provider will take the comments into account and provide an updated document within 5-10 working days. A specific deadline for reflecting the comments will be agreed for each document individually. The final result of the document is approved by the Contracting Authority.
<b>Acceptance procedure</b>	
Req. 465.	<p>The testing phase acceptance criteria:</p> <ul style="list-style-type: none"> <li>• Before the User Acceptance Testing (UAT) the Service Provider shall present a duly signed report on internal testing completed by the Service Provider confirming that the following was verified during the internal testing: <ul style="list-style-type: none"> <li>• Proper functioning of various Register functions and interfaces between them;</li> <li>• Proper functioning of the user interface;</li> <li>• Properly implemented functional and non-functional requirements;</li> <li>• Well-designed reports and documents.</li> </ul> </li> <li>• Before starting the UAT, shall provide detailed testing scenarios used to test the above requirements, specifying scenario steps, data and forms used in the scenario.</li> <li>• UAT must be successfully completed by the Contracting Authority according to the acceptance testing plan and testing scenarios drafted by the Contracting Authority, which will be deemed as completed if all steps of the scenario have been successfully implemented and meet the evaluation criteria, i.e., the expected result of each step of the scenario complies with the result of the Registry);</li> <li>• The UAT must be successfully completed within a maximum of three acceptance testing rounds of UAT and fix of identified errors;</li> <li>• All Critical issues must be resolved before the launch of the Registry (deployment to production environment);</li> <li>• Unresolved outstanding Medium errors must be no more than 3% of the total Medium errors recorded during the UAT, and the Service Provider must submit the time schedule for its fix;</li> </ul>

Reference	Description of Technical requirements
	<ul style="list-style-type: none"> <li>• Outstanding Minor unresolved errors/problems of the Registry (no more than 10% of the total Minor errors recorded during the UAT), and the Service Provider must submit the time schedule for its fix;</li> <li>• If the relevant documentation (specified in the Hand back requirements) is not prepared at the end of the UAT run, Registry (or its individual parts) is not considered complete and acceptable.</li> </ul> <p>Registry UAT will be completed, and Registry will be considered deemed for hand back (acceptance) when the results of all test scenarios meet the above test acceptance conditions.</p>
Req. 466.	<p>On the basis of the UAT testing plan provided by the Service provider and approved by the Contracting Authority, the Service provider of the Registry must physically participate in the Registry testing and provide consultations on how the Registry action/function/operation must be tested in accordance to the approved testing scenarios, which will be provided by the Service provider and approved by the Contracting Authority, to provide comments and suggestions on the recommended error criticality level, as well as to inform the testing participants about the error elimination deadline. All information about the error criticality level, the error elimination deadlines, the error elimination process and assigned responsible persons will be recorded in the error logging IT solution provided by the Service provider.</p>
Req. 467.	<p>The Service provider must perform the Registry performance testing in accordance with the Registry requirements. During the performance testing the Service provider of the Registry shall be responsible for creating the conditions for successful performance testing (e.g., the Service provider shall automatically generate the data required for performance testing, prepare automatic data upload means to be used during the performance testing etc.). The performance testing must be carried out in production (PROD) environment.</p>
Req. 468.	<p>The Service provider must resolve all the recorded errors and problems identified during the testing phase (both UAT and performance) in accordance with the information recorded in the testing error logging system and the error elimination plan. It will also be required to prepare a test report containing basic information on the errors recorded during testing.</p>
<b>Deadlines for completion of the Registry implementation</b>	
Req. 469.	<p>All stages of the Registry design and implementation from the signing of the Contract with the Service Provider to the launch of the Registry in the production environment (including the stages of project initiation, analysis, design, configuration (programming), UAT and preparation for the launch of Registry) must last no longer than 12 months.</p>
Req. 470.	<p>Registry implementation is considered completed when the Contracting Authority accepts all the results defined under specific phase and when the Service provider fulfils all the requirements and acceptance criteria set out in this technical specification</p>

### 3. ANNEXES

#### **Annex No. 1: Data about issued document volumes, enrolment / customer service facilities operated in Armenia and in foreign missions**

Attached document contains information about:

- General population statistics
- Information about enrolment / customer service locations and historical document volumes in Armenia
- Information about enrolment / customer service locations and historical document volumes in foreign missions

***[Attached as an excel document]***



3\_1\_Annex\_No\_1\_Statistical\_Information\_Dra

## Annex No. 2: Requirements for enrolment facilities characteristics

The arrangement of enrolment facilities shall correspond to the modern / renovated office and method of customer service with the goal to minimize the waiting and service time of citizens and residents. The table below provides the requirements for enrolment facilities, their location and network, as well as set-up.

No.	Requirements
<b>I. Enrolment facilities</b>	
1.	A new type of service station/workplace has to be introduced making it possible to handle all processes at the place of service effectively, discretely, facilitating mutual communication, paperless (or minimized) and comfortably (seated vs standing set up). Forms are filled/managed by operator.
2.	The facility is one space with a number of functional annexes
3.	Comfortable and spacious citizens waiting space with seats: <ul style="list-style-type: none"> <li>- Not less than 1,9 m2 per person in sitting area</li> <li>- 90 % of people waiting shall have seats available</li> </ul> The place of forced waiting will no longer have bad associations. In immediate proximity the monitors with relevant queuing and other information
4.	Citizens and residents servicing is orchestrated through online registration and on-site queuing and customer feedback system
5.	The colors of the arrangement refer to the national colors of the country
<b>II. Location and network of enrolment facilities</b>	
6.	At least one enrolment facility per regional center in Armenia
7.	Located not far from the city or municipal center in a convenient location easy to reach by private and public transport
8.	At least 2 dedicated parking spaces for disabled next to the facility
9.	Dedicated or public parking spaces (for other than disabled citizens) must be available not further than 3 min walking distance
<b>III. Set-up</b>	
9.	Disabled people access
10.	Service station/workplace must be introduced making it possible to handle all processes (application, biometric data capturing, payment, etc.) at the place of service
11.	Dedicated service places for disabled
12.	8-12 m <sup>2</sup> per one service station/workplace
13.	Dedicated waiting area with seats and immediate proximity to information monitors
14.	On-site queuing system - one per enrolment facility
15.	Safe storage of produced passports and IDs (fire and waterproof)
16.	24-hour indoor and outdoor surveillance system

No.	Requirements
17.	Intrusion and fire alarm system connected to security services, physical security during working hours in city offices
18.	Sanitation facilities separated for males and females on or near the premises
19.	Air Quality, Thermal Environment, Lighting and Acoustics conditions meeting standard “EN 15251: Indoor Environmental Input Parameters for Design and Assessment of Energy Performance of Buildings Addressing Indoor Air Quality, Thermal Environment, Lighting and Acoustics” or its equivalent
20.	Category A - Yerevan and other large cities’ passport office (multiple workplaces, dedicated facility, kids’ zone, etc.)
21.	Category B - municipal center outlets (few workplaces, could be established as part of multifunctional facility - post, police, etc.)
22.	All furniture and office equipment necessary for the provisioning of services

### Annex No. 3: Estimated services' volumes

#	Document	Type	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total
<b>I</b>	<b>Biometric passports</b>												
1	Biometric Passport of the citizen of the Republic of Armenia (Regular)	T3	222 222	222 222	222 222	222 222	222 222	222 222	222 222	222 222	222 222	222 222	2 222 220
2	Biometric Passport of the citizen of the Republic of Armenia (Diplomatic)	T3	556	556	556	556	556	556	556	556	556	556	5 560
3	1951 Refugee Convention Travel Document	T3	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	11 110
4	1954 Stateless Persons Convention Travel Document	T3	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	11 110
5	Service Passport of the citizen of the Republic of Armenia	T3	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	1 111	11 110
			226 111	226 111	226 111	226 111	226 111	226 111	226 111	226 111	226 111	226 111	2 261 110
<b>II</b>	<b>eID cards</b>												
6	Electronic Identification Card of the citizen of the Republic of Armenia	ID1	411 111	411 111	411 111	411 111	411 111	537 779	537 779	537 779	537 779	537 779	4 744 450
7	Residence Permit Electronic Card of the Republic of Armenia	ID1	11 111	11 111	11 111	11 111	11 111	22 222	22 222	22 222	22 222	22 222	166 665
8	Non-Residents and Foreign Citizens Electronic Identification Card of the Republic of Armenia	ID1	1 111	1 111	1 111	1 111	1 111	2 222	2 222	2 222	2 222	2 222	16 665



#	Document	Type	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total
9	Refugee's Electronic Identification Card of the Republic of Armenia	ID1	1 111	1 111	1 111	1 111	1 111	2 222	2 222	2 222	2 222	2 222	16 665
10	Stateless Persons Electronic Identification Card	ID1	1 111	1 111	1 111	1 111	1 111	2 222	2 222	2 222	2 222	2 222	16 665
11	Foreign Diplomats Electronic Identification Card	ID1	556	556	556	556	556	1 111	1 111	1 111	1 111	1 111	8 335
			426 111	426 111	426 111	426 111	426 111	567 779	567 779	567 779	567 779	567 779	4 969 450
III	Specimens and tests												
12	Specimens	ID3	2 500										2 500
13	Specimens	ID1	3 000										3 000
14	Test (white cards with electronic functionalities)	ID1	100	100	100	100	100	100	100	100	100	100	1 000
			5 600	100	100	100	100	100	100	100	100	100	6 500

#### **Annex No. 4: Minimum Security Principles**

This appendix is an integral part of the minutes of the meeting No. 05/2022 of December 27, 2022 of the Information Systems Management Council.

The appendix defines the minimum security principles for the implementation of the new system of RA biometric passports and identification cards, based on the full-service outsourcing model.

1. All processes of the current management of the passport decision making system shall be carried out under the direct control of the MIA/Government, without the participation/presence and control of the MIA/Government the vendor will not have access to the existing system for software-hardware updates, replacement and maintenance. The management and maintenance of biometric data and document repositories and servers is not outsourced and should be carried out exclusively by the MIA/Government. Management and maintenance of temporary (cache) data and servers supporting the process of providing services is carried out under the supervision of the Police.
2. Outsourced services are provided by a legal entity registered in the Republic of Armenia, which will be established by the company that won the tender or will participate in the tender as a consortium.
3. All software and equipment (except equipment installed in diplomatic missions) is physically located in Armenia, in Government controlled areas. Additionally, printing equipment and servers are located exclusively in MIA/Government owned premises.
4. All network regulations and restrictions are implemented by the Government. Devices for collecting personal data and receiving applications in foreign countries are connected to the central system in a manner approved by the Government.
5. The printing of passports is carried out in the administrative area of the MIA, under the supervision of MIA employees. The process of storing and managing the blanks is carried out with the physical presence and control of the MIA officer, including provided with appropriate technological solutions.
6. Strict quality and safety control is imposed by the MIA/Government in service offices.
7. A group of specialists is formed in the MIA/Government for the technical works defined by this annex (management and maintenance of infrastructure (databases) containing biometric and personal data, management and maintenance of their server infrastructure, etc.), as well as quality control and contract management/supervision to perform functions.
8. Repositories and servers of biometric data and documents are under the management and control of the Government. The server area is operated and maintained by the Police/Government.
9. The population register is not the subject of an outsourcing tender, and the system's relationship with it is carried out through the interoperability platform in the same way as for all other users.
10. The winner of the competition is obliged to ensure the best international standards, their certification and independent audit.
11. Data in databases and during exchange are at least subject to encryption, as well as other security methods are used. Access authorization keys are provided and controlled exclusively by Government/Police professionals.
12. The Source Code of the entire software package should be made accessible to GoA for validation / audit by Government/MIA professionals or a specialized organization before the system is implemented and operational.

## Annex No. 5: Minimum Requirements for Asset Hand back

### General Requirements applicable to all assets

1. Comprehensive inventory verification (please see below in the table asset categories subject to inventory) shall confirm that all assets (incl. Movable Property, Intangible Assets) acquired for the performance of the contract are accounted for and handed over as specified and broken / damaged, and obsolete items (assets with remaining lifetimes shorter than defined in this document) are replaced. Inventory shall provide the following information: acquisition date, deployment date, initial purchase value, depreciated value, remaining useful lifetime (when available evidenced by Manufacturer's Warranty, Product Specifications, Service Contracts, Industry Standards or similar impartial information sources).
2. Assets shall meet all the requirements applicable as per Technical Requirements.
3. All requirements detailed in chapter "2.6.3 of Technical Requirements on Hand back requirements", incl. but not limited to requirements on Training, Documentation, Licensing conditions, Warranty service, shall apply.
4. Detailed maintenance records shall be provided for assets, demonstrating that it has been adequately maintained throughout the duration of the PPP contract, broken or damaged items have been replaced, any software updates, upgrades, or modifications made documented.
5. Assets shall be presented in a clean, presentable condition, free from any damage or defects beyond normal wear and tear, structural defects, and safety hazards, with landscaping, parking areas, and common areas in good condition. All assets operate correctly and efficiently.
6. All necessary documentation, including but not limited to building plans, permits, warranties, user manuals, servicing schedules, patents, copyrights, trademarks, software licenses, and proprietary processes shall be provided to the entity taking over the assets.
7. All assets subject to handover shall be warranted for a period of one year from the date of handover. The warranty shall cover all defects that arise during normal use of the asset and is evidenced to be the fault of improper implementation of the PPP agreement. The Service provider shall, at their discretion, either repair or replace the asset, or provide a refund, free of charge, for any defective parts or the entire asset during the warranty period.

### Asset category specific requirements (additional to General Requirements)

Asset Category			Asset Category specific Minimum Requirements for Hand back
Rented Real Estate	Enrolment facilities		<ol style="list-style-type: none"> <li>1. The facilities to extent it is applicable and defined in the technical requirements shall be in compliance with the latest security standards (PCI CP, ISO27001, eIDAS requirements) at the moment of the Hand back.</li> <li>2. The property must comply with all relevant building codes, zoning regulations, environmental standards, and health and safety requirements.</li> </ol>
Transferred Real Estate	Personalization facility		
	Data center facility		

Asset Category			Asset Category specific Minimum Requirements for Hand back
	Disaster recovery facility		<ul style="list-style-type: none"> <li>3. Training and support must be provided to the new operator to facilitate a smooth transition and effective management of the property.</li> <li>4. Access to essential utilities and services, including water supply, electricity, heating, cooling, and waste management, must be ensured. All related contracts must be handed over with no outstanding debt.</li> <li>5. All operational systems within the property, such as HVAC, electrical, plumbing, and fire safety systems, must be fully functional.</li> </ul>
Movable Property	Furniture	Furniture placed in enrolment facilities	-
		Furniture placed in personalization facility	
		Furniture placed in Data center facility	
		Furniture placed in Disaster recovery facility	
	Basic work-station equipment (computers, payment card readers, etc.)	Work-station equipment placed in enrolment facilities	-
		Work-station equipment placed in personalization facility	
		Work-station equipment placed in Data center facility	
		Work- station equipment placed in Disaster recovery facility	

Asset Category			Asset Category specific Minimum Requirements for Hand back
	Hardware / equipment to support core processes	Hardware placed in enrolment facilities (stationary or movable)	6. Remaining useful lifetime of hardware / equipment must be not less than 3 years, proofed by Manufacturer's Warranty, Product Specifications, Service Contracts, Industry Standards or similar impartial information sources.
		Hardware placed in personalization facility	
		Hardware placed in Data center facility	
		Hardware placed in Disaster recovery facility	
	Document blanks	Document blanks – empty	7. Evidence that all ordered / produced blanks are handed over. 8. Stock of document blanks stored in Armenia is not less than average expected document demand for 1 year.
		Document blanks – personalized	
	Minor office supplies	NOT SUBJECT TO INVENTORY	-
Intangible assets	Software	Software to support enrolment and personalization processes: <ol style="list-style-type: none"> <li>1. Citizen eService application (web portal)</li> <li>2. Enrolment solution</li> <li>3. Identity management and document issuance solution</li> <li>4. Documents and biometric data registry / database</li> <li>5. Automated Biometric Identification Solution (ABIS)</li> <li>6. Personalization solution</li> <li>7. ICAO/EAC Public key infrastructure</li> <li>8. On-site queuing management solution</li> <li>9. Reports and statistics solution</li> <li>10. Integrations with external data sources</li> </ol>	<ol style="list-style-type: none"> <li>9. Ensure continuity of use and access to the intangible assets, including transfer of any necessary software licenses, subscriptions, or access rights, to prevent disruptions in operations.</li> <li>10. All software license versions must be supported by manufacturer for not less than 3 years after handover, proofed by Manufacturer's Warranty, Product Specifications, or similar impartial information sources.</li> <li>11. Verification that the ownership and validity of all intangible assets transferred, including confirming that they are free from any encumbrances or legal disputes.</li> <li>12. Comprehensive documentation of all assets, including patents, copyrights, trademarks, software licenses, and proprietary processes, is provided to the entity taking over.</li> <li>13. All non-proprietary software source code must be handed over and stored in the repository indicated by the Contracting Authority.</li> </ol>

Asset Category			Asset Category specific Minimum Requirements for Hand back
		Software to support data center and disaster recovery sights	14. All proprietary source code must be stored in an escrow account. The escrow agreement between the depositor/owner of the source code, Contracting Authority and the escrow agent must be signed before commencement of the operational phase and must be maintained for the duration of the Contract and 1 year after hand over.
		Enterprise software (MS Office, etc.)	
	Other intangibles (e.g., patents, copyrights, trademarks, proprietary processes, etc.)		

## **Annex No. 6: Requirements for depositing proprietary software source codes in Escrow account**

1. Subject to point 2 below, the Service Provider shall put a copy of the software source code and associated materials (Material) for secure storage within escrow account prior to the Commencement Date. The deposited Material shall remain the confidential and intellectual property of the Service Provider or its licensors.

The Material shall contain all information in human readable form necessary to enable a reasonably skilled programmer or analyst to maintain and, in case of non-standard (non-licensed) software build for project purposes, enhance the software, and without prejudice to the generality of the foregoing, that the source code and related documentation shall contain all listings of programmers' comments, data and process models, logic manuals, and flowchart. It should also include configuration, installation and operation guides (files), dependencies and testing scripts per type of software.

2. However, the Service Provider may deposit sensitive Materials, including cryptographic and biometrics components, embedded software (identity card OS & Applet), core biometrics engine and proprietary software components, within escrow account in their executable form only (compiled for the specific platform used in the production environment).
3. Materials subject to security certifications may not be deposited into an escrow account.
4. Third-party utilities (COTS), including but not limited to Microsoft and Oracle, shall be listed along with their respective versions to clearly specify the licenses or utilities that must be procured by the Contracting Authority in the event the software in the escrow account is released according to point 5 below. Such third-party utilities shall not be part of the Materials to be put in the escrow account.
5. The Service Provider acknowledges that the Contracting Authority exclusively for continuity of the Services and Operations may require access to the Material, if:
  - 5.1. the Service Provider ceases its business for more than 22 Business Days without assigning its rights and obligations under the escrow agreement to a third party (excluding the cessation of business for any excusable reasons under the Agreement or Applicable Law, including Force Majeure or Political Force Majeure); or
  - 5.2. the liquidation procedure in relation to the Service Provider, judicial bankruptcy proceedings or any other proceedings related to insolvency of the Service Provider is initiated; or
  - 5.3. the Service Provider assigns (with the notification to the Contracting Authority of such assignment) its intellectual property rights to the Material to a third party which fails, within 60 days of all parties' knowledge of such assignment, to continue escrow protection for the benefit of the Contracting Authority by failing to either transfer the escrow agreement or this Agreement to the assignee; or enter into a new escrow agreement which offers the substantially similar protection.
6. The Service Provider agrees that third party acting as an escrow agent shall be allowed to release to the Contracting Authority the Materials in cases indicated in point 5. Before depositing the source code to the escrow account, the parties shall conclude a three-party escrow agreement with the escrow agent company selected according to point 9 below including, in particular, the release conditions defined in point 5 above.

7. The Service Provider warrants to the Contracting Authority that the Materials are sufficient to enable a qualified person to continue provision of the Services and Operations.
8. The Contracting Authority warrants and represents to the Service Provider, that it shall use the Materials made available according to point 5 above solely in connection with the provision of the Services and Operations.
9. The escrow agent company will be selected by the Service Provider and vetted by the Contracting Authority.
10. Escrow account costs will be borne by the Service Provider.
11. The obligations of the Service Provider specified here shall expire upon expiry of the warranty specified in chapter "2.6.3. Hand back requirements". Correspondingly, the term of the escrow agreement shall be limited to this period. After expiry of the escrow obligations of the Service Provider according to this clause, the Materials put to the escrow account shall be returned to the Service Provider.