TERMS OF REFERENCE

for the creation
of the Information System of electronic apostille
and electronic register of certified documents
E-App and E-Register

Contents

Introduction

This Terms of Reference is intended to describe the composition of the requirements for the creation of an Information System for an electronic apostille and an electronic register of certified documents "E-App" and "E-Register" (hereinafter - IS).

IS combines the functionality of "E-App" and "E-Register" and considers them together. IS has a unified database for the Republic of Uzbekistan.

1. General information

1.1. Full name of the IS and its symbol

Full name of IS: Information system of electronic apostille and electronic register of certified documents.

Short name: "E-App" and "E-Register".

Symbol: ISEAER (hereinafter referred to as IS, System).

1.2. Name of the organizations of the customer and the developer of the IS

The client of the IS is: UNDP in Uzbekistan.

The beneficiary of the IS is the Public Services Agency under the Ministry of the Republic of Uzbekistan

Address: Tashkent, A. Temur street - 16 A.

Telephone: 71 207-00-66

E-mail: info@davxizmat.uz

The contractor for the development of the IS will be determined based on the results of the tender (competitive) bidding.

1.3. List of documents on the basis of which the IS is created

List of documents based on which the IS is created:

- Decree of the President of the Republic of Uzbekistan "On measures to radically reform the national system of providing public services to the population" No.UP5278 dated 12.12.2017.
- Resolution of the President of the Republic of Uzbekistan “On Measures to Implement the Provisions of the Convention Abolishing the Requirement of Legalization of Foreign Official Documents (HAGUE, October 5, 1961) No. PP1566 dated July 5, 2011.
- Resolution of the Cabinet of Ministers of the Republic of Uzbekistan "On further improvement of the procedure for affixing an apostille on official documents"

1.4. Planned start and finish dates

Planned dates for the start and end of work on the creation of IS:

Start – May 2021;

Completion - September 2021.

1.5. The procedure for registration and presentation of the results of work

The registration of the results of work must comply with the requirements set forth in the following regulatory documents:

1. O'z DSt 1985:2018 Information technology. Types, completeness and designation of documents when creating information systems;
2. O'z DSt 1986:2018 Information technology. Information Systems. Stages of creation;
3. O'z DSt 1987:2018 Information technology. Terms of reference for the creation of an information system;
4. O'z DSt 1047:2018 Information technology. Terms and Definitions. The following scope of work has been determined:
    1. Development of Terms of Reference for IS;
    2. Passing the examination of the Terms of Reference in the State Unitary Enterprise "Center for Electronic Government Project Management" of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan;
    3. Passing the examination of the Terms of Reference at the State Unitary Enterprise "Cybersecurity Center" under the State Security Service of the Republic of Uzbekistan;
    4. Holding a tender and concluding a contract for the development of IS;
    5. Development of IS software;
    6. Testing and, if necessary, revision of the IS;
    7. Drawing up operational documentation on IS;
    8. Examination of the software product for compliance with the Terms of Reference in the State Unitary Enterprise "Center for Management of Electronic Government Projects" of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan;
    9. Examination of the software product for compliance with security requirements at the State Unitary Enterprise "Cybersecurity Center" under the State Security Service of the Republic of Uzbekistan;
    10. Conducting trainings, including providing technical support and support for the developed IS software;
    11. Launching the IS into operation. Based on the results of this stage of work, the

Developer submits to the Customer the Certificate of Completed Work, and the Certificate of IS commissioning is signed.

The software development stage will be divided into steps as agreed by the Customer and the Contractor. A detailed development schedule will be an annex to the Agreement between the Customer and the Contractor. Based on the results of each stage of development, the Contractor and the Customer will sign the Certificate of Completion.

It is preferable to split the development into functional modules in accordance with the list of subsystems given in Section 4.1.1. of this Terms of Reference, indicating the timing of the development of each stage. Development stages (subsystems) will be accepted by the Customer sequentially.

1.6. Terms and abbreviations

1.6.1.Abbreviations

In this Terms of Reference, the following abbreviations are used:

PSA - Public Services Agency under the Ministry of Justice of the Republic of Uzbekistan

DI - Database of individuals

DL - Database of legal entities

Single Portal – Single portal of interactive government services;

UIS - Unified information system for identification of users of the Republic of Uzbekistan;

IS - Information System, in this document is used as a designation of hardware and software for the implementation of the functions "E-App" and "E-Register";

Convention - Hague Convention Abolishing the Requirement for Legalization of Foreign Public Documents, October 5, 1961;

UNDP – United Nations Development Program;

ToR – Terms of Reference;

EDS – electronic digital signature.

1.6.2.Terms

In this ToR, the following definitions are used:

Apostille - a special stamp affixed to an official document for use abroad in accordance with the Convention, confirming the authenticity of the signature of the person who signed the

document and the seal or stamp certifying the document;

Competent state body - A state body authorized to affix an apostille in accordance with the Decree of the President of the Republic of Uzbekistan dated July 5, 2011 No. PP-1566 "On measures to implement the provisions of the convention abolishing the requirement of legalization of foreign official documents (HAGUE, October 5, 1961)" ;

Module - a fragment of the developed information system, covering a set of logically related functions.

Personal account - a resource that displays a collection of user data, where the user can send applications for an apostille**.**

Subsystem - a functional part of the developed IS, which includes modules and some objects.

Apostille affixing - is an official procedure required to confirm the authenticity of the signature of the person who signed the document and the authenticity of the seal or stamp confirming the document.

Technological instruction - a technical instruction describing the procedure for interaction at the API level (application programming interface) with information systems external to the developed IS;

"E-App" - is a software product that creates a special electronic stamp on an official document in accordance with the Convention, which confirms the authenticity of the signature of the person acting as a signatory and the authenticity of the seal or stamp certifying the document.

"E-register" - a register containing a list of documents approved by the competent state body in the manner prescribed by law, used to verify these apostilles.

2. Purpose and goal of the creation of the IS

2.1. Purpose of the IS

The purpose of the IS is to automate the procedure for the provision of public services for affixing a special stamp "Apostille" on official documents issued in the territory of the Republic of Uzbekistan.

Applications for an electronic apostille are accepted through Single Portal and public service centers. The IS will allow the introduction of a completely new procedure for apostille of official documents in the country and will also allow the use of the E-App software for filing documents for apostille and E-register for verifying the authenticity of the apostilled documents contained in the

register via the Internet.

The information system being created will make it possible to create tools for working with apostilles issued in the Republic of Uzbekistan using information and communication technologies.

The IS will be posted on the resources of the PSA.

2.2. The goal of creating the IS

The goal of the project is:

- Creation of a unified register of ministries and departments involved in affixing apostilles (100% registration of all incoming documents in a single register).
- Attracting individuals and legal entities to obtain an apostille in a new format.
- Improving the quality of public services, reducing duplication of documents, eliminating bureaucratic barriers in obtaining services.
- Reducing the time for checking apostilles (up to 3 days).
- Obtaining statistical information on issued apostilles (according to all information in the database).
- Control over the provision of public services of affixing an apostille.
- Translation into electronic form of the state service for affixing an apostille (the possibility of obtaining an apostille both in electronic and paper form, with the obligatory entry into the register).
- Abolition of redundant administrative procedures.
- Creation of an online payment mechanism for the state service of affixing an apostille.

Achievement of the set goals of the project is assumed using a unified approach and standards for the implementation of information and telecommunication technologies as a result of solving the following project tasks:

- Formation of a single database of apostilles and tools for working with the database.
- Creation of tools for submitting documents for obtaining an electronic apostille.
- Creation of electronic apostille authentication tools (100% collection in the register of all certified signatures, seals and stamps).

- Creation of a system of interaction between participants in the process of providing services for obtaining an electronic apostille.
- Creation of opportunities for obtaining services for obtaining and verifying the apostille through the Single Portal (digitalization of information exchange between all involved authorities).
- Creation of tools for obtaining statistical information regarding apostilles issued in the Republic of Uzbekistan.
- Creation of tools for making payments for services of affixing an apostille.

3. Characteristics of the object of informatization

3.1. Short information about the objects of automation.

Currently, there are no information systems in the Republic of Uzbekistan that fully or partially perform the functions of issuing an electronic apostille.

To obtain a public service for affixing an apostille, the applicant applies to the Public Services Center, or to the responsible organization with notarized copies and translations of the documents to be apostilled.

Agencies responsible for apostilling:

- Supreme Court
- Ministry of Foreign Affairs
- Inspection for Quality Control of Education under the Cabinet of Ministers.
- Territorial administrations of justice
- General Prosecutor's Office.

The applicant must pay the state fee for the use of the service, and then, upon the expiration of the specified period, receive a ready-made apostille.

Apostille is issued by placing a stamp on the document (or on a notarized translation of the document).

In order to verify the authenticity of the apostille, the person concerned must contact the appropriate authority to obtain information about the apostille.

This process takes quite a long time both for the registration and for the verification of the authenticity of the apostilles. At the same time, information about the affixed apostilles is stored in

scattered non-digital sources, which complicates the collection of information, its processing and analysis. The process of interaction between departments is also not automated, which creates difficulties in obtaining timely data.

The development of the information system is carried out in order to create a single virtual space to increase information support for the population and stakeholders, including foreign stakeholders.

3.2. Information about the operating conditions of automation objects and characteristics of the environment

Объекты автоматизации располагаются, как правило, в достаточно комфортных помещениях, не подверженных каким-либо вредным воздействиям и удовлетворяющих основным нормам охраны труда и техники безопасности персонала, и требованиям по установке средств вычислительной техники.

3.3. Processes to be automated

The following processes are subject to automation through IS:

- Submission of documents for obtaining an electronic apostille;
- Payment of the fee;
- Verification of the identity of the signature, seal and stamp on the submitted document with signatures, seals and stamps contained in the IP database;
- Checking the status of consideration of documents (responsible department, status);
- Formation of a unique QR-code of the apostille;
- Receipt of notifications by the applicant when the apostille is ready
- Apostille signing with EDS;
- Online apostille authentication using a QR code;
- Viewing apostille data (in pdf format, with two attachments: verification of authenticity, as well as the document itself);
- Formation of statistics on apostilles
- Control over the provision of public services of affixing an apostille.

IS implies user access to the system in the "client-server" mode, using Web technologies.

4. General requirements

4.1. Requirements for IS in general

4.1.1. Requirements for the structure and functioning of the IS

Open-source software should be used as a platform for building the IS.

The IS design should be based on a service-oriented architecture:

- level of information presentation
- applied business logic level
- the level of transportation of services
- data storage and processing layer (database server)

The IS should take into account:

- ensuring the security of access to data stored in the IS database
- organization of the user's personal account
- organization of strict delimitation of user access to various functions, depending on their competence, position held, and powers assigned to them
- providing logging at the database level of all events carried out through the functionality of the IS (logs)

The IS functionality should maximally realize the set goals, be scalable and readable. The IS must include the components described in the table below.

4.1.1.1. List of IS modules, their purpose, and main characteristics

Table 1. List of subsystems and their purpose.

№	Name	Description
1.	User authorization module	A module for identifying users (applicants) in the system. Provide authorization through One-ID for individuals, as well as through the use of EDS for legal entities. Authorization must be available through Single Portal.
2.	Authorization module for departments/agencies	Authorization of the responsible authorities is intended for: • The Supreme Court • The Ministry of Foreign Affairs • Inspection for Quality Control of Education • Territorial Departments of Justice • General Prosecutor's Office Also, access should be organized for employees of the

№	Name	Description
		Public Services Agency to receive applications, monitor the provision of public services and monitor the system's performance. Authorization must be carried out using an electronic digital signature in accordance with the international standard.
3.	Administrator authorization module	The administrator authorization module implies access to the system using a dedicated administrator login and password.
4.	Storage module for signatures and seals	The system should allow storing and using digital and graphic signatures (signatures and seals), keeping records of them, allowing to control the terms of their use in accordance with the regulations. Also, the module should allow comparing the signatures of apostilled documents (scans) and seals, stamps of the organizations that issued them, and determine compliance.
5.	User account	Designed to provide the user with the ability to work with electronic apostilles, including the functions in clauses 4.1-4.4.
5.1.	Application generation module	Formation of an application for an Apostille (one document or a package of documents)
5.2.	Module for adding scanned versions of documents	Adding scanned versions of documents, as well as notarized translations.
5.3.	Application status check module	The user must be able to: • Viewg pending applications • Check the status of the application • Receive notifications by review statuses
5.4.	Apostille upload module (E-Apostille)	The user must be able to: • Downloading of Apostille and printing it in .pdf format. • Viewing the history of applications and review results.
6.	Departments Account	Each department must receive applications in accordance with the rules for consideration. The cabinet includes the functions of peragraphs 6.1-6.7
6.1.	Document queue module	The module involves working with a queue of documents for consideration to obtain an Apostille.
6.2.	Dossier Module	The module should provide the ability to view the Dossier of all the documents under consideration.

№	Name	Description
6.3.	Stock module	The module must be able to view rejected applications.
6.4.	Signed documents module	The module assumes working with signed documents, including viewing, searching through them.
6.5.	Search module	Advanced search for documents, including the ability to filter documents by types, by approving employees, by territorial affiliation, by the date of the Apostille affixing, by the applicant's last name, by country of departure and other possible parameters.
6.6.	Monitoring module for the provision of public services	This module allows PSA employees to monitor the provision of public services
6.7.	Statistics module	It provides for the formation of statistical data on the volume of applications issued by Apostilles, as well as in the context of departments, countries / regions / districts, individuals / legal entities, etc.
7.	Administrative module	System administration and system data management is carried out by an administrator
7.1	Role management	The control unit for user roles and access allows you to assign specific roles to users.
7.2	Access matrix	The Access Matrix block allows you to configure the differentiation of user roles' access to system data.
7.3	References	Block for managing directories and classifiers of the system.
7.4	Logs	Block for viewing the system event log
7.5	Service monitoring	System health control unit
7.6	Help	The block for the formation of reference materials on the work of the system, tips for users.
7.7	Notifications	Block for generating notifications to users.
8.	Apostille information request module	The module is intended for access by external partners, interested parties to check the status of the Apostille (relevance and validity) and the main details of the issued Apostille, as well as scanned versions of documents.
9.	Integration module	For integration with external systems. The first stage implies integration with the Single Portal, SPC, Ministry of Internal Affairs, State Tax Committee, Single authorization system with an SMS gateway for sending notifications to users, payment systems. It also provides for integration with the EDS Key

№	Name	Description
		Registration Center (Unicon), the Register of Reference Books and Classifiers.
10.	Payment processing module	Payments can be made by interacting with functioning payment systems in the Republic of Uzbekistan (Click, Payme, Upay, Paynet).
11.	E-register backend	It is intended for processing all system functions, queries to the database, processing queries on the interaction interfaces (API), both within the system and to external systems.

The structural diagram of the IS is shown in the figure below.

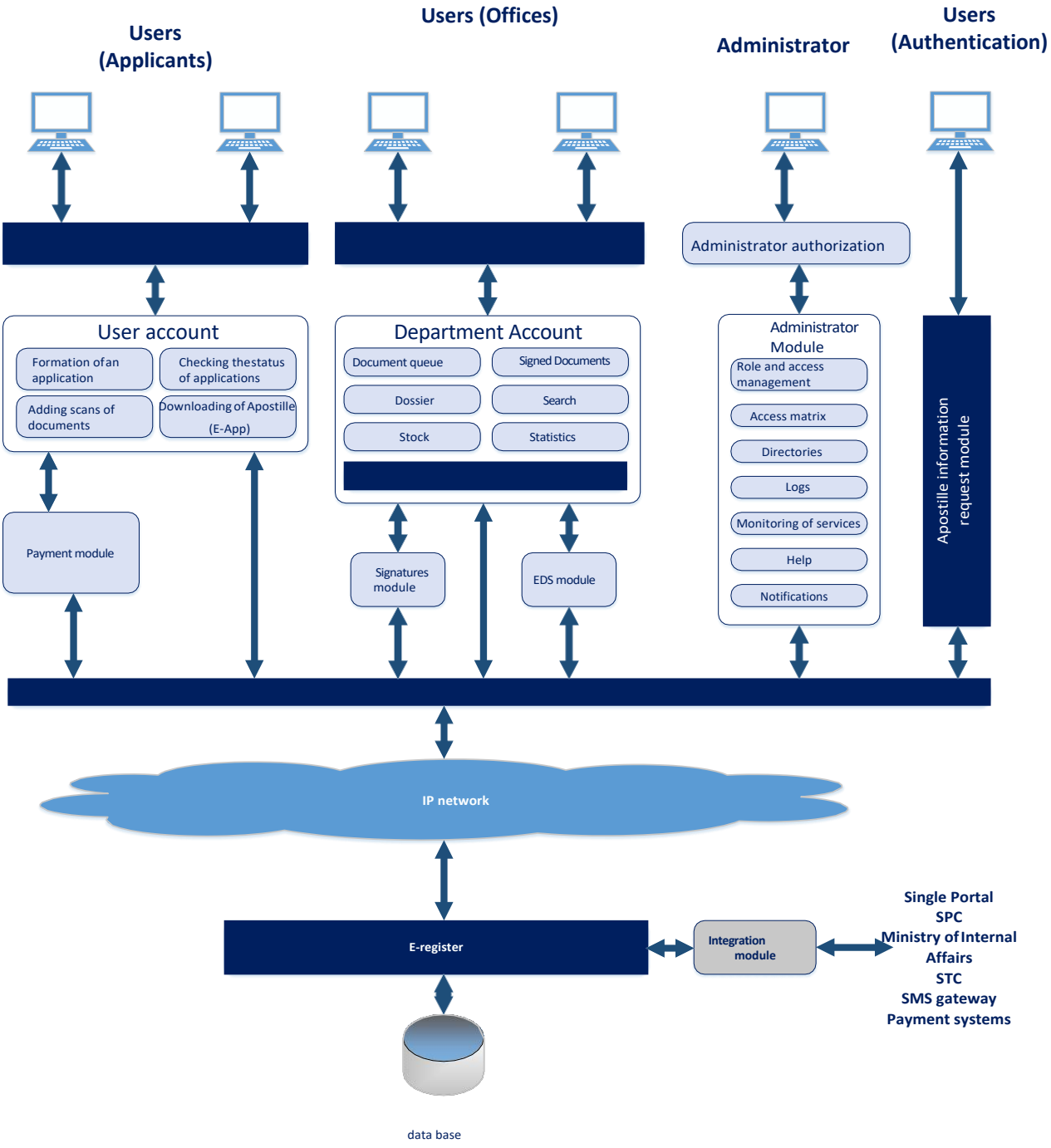
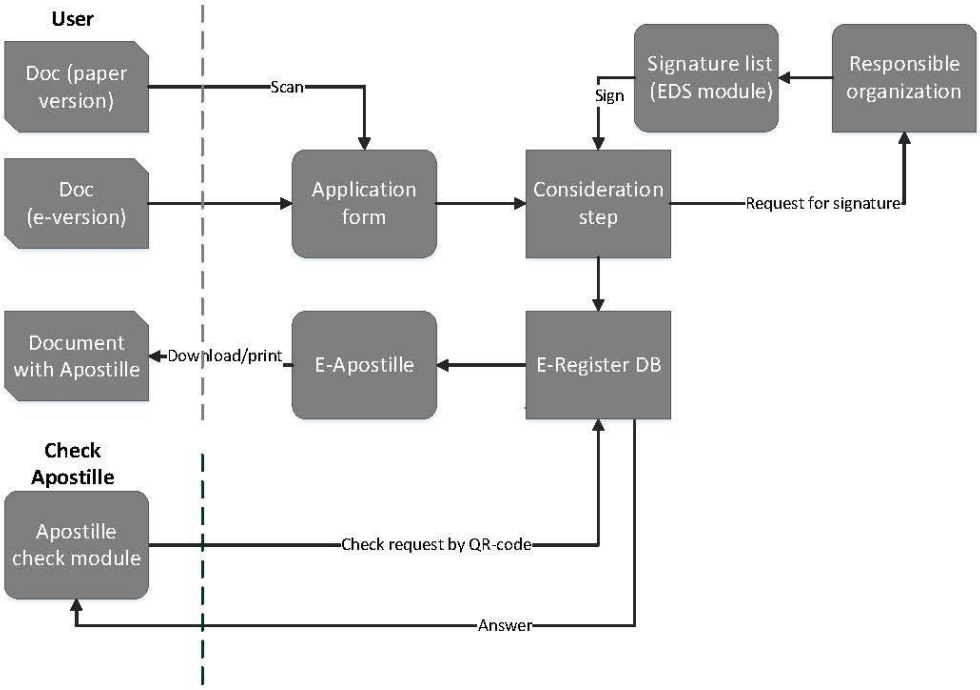


Figure 1. IS block diagram.

The logical scheme for issuing an electronic apostille is shown in the figure below:



1. The applicant submits a document (a paper document must be scanned, an electronic document will be attached to the application and uploaded into the system).
2. The applicant (individual or legal entity) fills out the application form at the Single Portal.
3. At the stage of consideration, the system sends an application to the responsible organization in accordance with the Regulations.
4. The responsible officer of the department checks the documents and puts an approving electronic signature (previously saved in the system signature registry).
5. The document is saved in the "E-register" database.
6. An organization or any interested user, both in the Republic of Uzbekistan and abroad, who wants to check the Apostille by QR code, sends the request through a special form Apostille check. The request is sent to "E-register", from where the response is returned. When checking by QR code, all information, and details of the requested Apostille must be provided. The module should also allow checking the Apostille by the entered number and date of issue.

4.1.1.2. Requirements for the modes of functioning of the IS

For the IS, the following modes of operation are defined:

- normal mode of operatio
- emergency operation mode

The main mode of operation of the IS is the normal mode.

In the normal mode of operation of the IS:

- The portal operates around the clock, seven days a week
- server software and technical means of the servers provide the possibility of round-the-clock operation, with breaks for service

To ensure the normal functioning of the IS, it is necessary to fulfill the requirements and maintain the operating conditions of the system, the versioning of the end user devices, as well as the complex of the IS hardware specified in the relevant technical documents (technical documentation, operating instructions, etc.).

The emergency mode of functioning of the IS is characterized by the failure of one or more components of the software and (or) hardware.

In the event of a transition to the emergency mode, the IS should provide the ability to terminate the work of all user sessions with the preservation of data.

Emergency mode actions:

- diagnosing incidents or problems associated with failures or abnormal situations in the operation of the IS
- restoration, if necessary, of the software and hardware configuration of the IS (network and server equipment)
- recovery of information in case of its loss by means of the backup and recovery system
- investigating the causes of the emergency and determining the causes of the incident or problem.

Responding to abnormal situations includes alerting maintenance personnel, taking measures to eliminate the problem, the necessary recovery of information, and the development and implementation of preventive measures.

4.1.1.3. List and description of use cases

This section lists the main scripts used in the system. All possible auxiliary scripts that support the logic of the system operation can be implemented at the discretion of the Contractor in accordance with the functionality described in section 4.2. of this Terms of Reference.

The main use cases in the system are:

- Registration of an application for apostille (C-01-01)
- Payment of the application (C-01-02)
- Consideration of apostille (C-01-03)
- Verification of the authenticity of the signature, seal and stamp on the submitted document with signatures, seals and stamps contained in the IS database (C-01-04);
- Apostille authentication (C-01-05)
- Adding scanned documents (C-01-06);
- User authorization in the system by means of One-ID (C-01-07);
- User authorization in the system by means of digital signature (C-01-08);
- Checking the status of the application (C-01-09);
- Unloading apostille documents from the system (C-01-10);
- Formation of statistical reports (C-01-11).
- Apostille signing with EDS (C-01-12);
- Authorization of the administrator in the system (C-01-13)

Registration of an application for an apostille

Use case number: *C-01-01*

Launch conditions: User launch of the application filling functionality.

Process owner: Applicant / employee of the Central State University or the responsible body.

Use case execution order:

1. Launching the application filling functionality
2. Filling in all parameters of the application by the user
3. Adding scanned versions of documents to the application (C-01-06)
4. Execution of the payment execution use case (C-01-02)
5. Saving the application
6. Submission for consideration

7. Complete the use case

Use case execution time: *the execution time of this scenario is not regulated by the System, depends on user actions*.

Input data: *Application data****.***

Output data: *Application identifier, data for consideration****.***

Possible IS extensions: *additional security checks for user credentials****.***

Payment for the application

Use case number: *C-01-02*

Launch conditions: Use case C-01-01;

Process owner: Applicant;

Use case execution order:

1. Launch of the payment processing functionality
2. Formation of the amount of the state fee
3. Choosing a payment system for payment
4. Go to the website of the payment system to make a payment
5. Receiving payment data from the payment system
6. Saving payment information in the database
7. Return to use case C-01-01 to complete work with the request.

Use case execution time: *the execution time of this use case is not regulated by the System, it depends on the actions of users.*

Input data: *Application ID, payment amount, payment system ID.*

Output data*: Payment data.*

IS extensions: *in the course of operation, the list of payment systems can be expanded.*

Consideration of apostille

Use case number: *C-01-03*

Launch conditions: completion of use case C-01-01;

Process owner: responsible officer

Use case execution order:

1. Receiving an application for consideration
2. Review of all documents and application data (conducting review activities)
3. Verification of the authenticity of the signature, seal and stamp on the submitted document with signatures, seals and stamps contained in the IS database (C-01-04)
4. In case of authenticity, creation of an apostille for the document
5. Signing a document using EDS (using Unicon Key Registration Center) (Scenario C-01-12);
6. Completion of the use case.

Use case execution time: *the execution time of this use case is not regulated by the System, it depends on the user's actions*

Input data: *Application ID and data*

Output data: *Apostille*.

Scenario extensions: in terms of searching for information and considering applications, the system should provide a convenient interface for dividing applications into categories: Dossier, stock, signed documents, search, monitoring of service provision.

Verification of the authenticity of the signature, seal and stamp on the submitted document with signatures, seals and stamps contained in the IS database

Use case number: *C-01-04*

Launch conditions: execution of use case C-01-03;

Process owner: responsible officer

Use case execution order:

1. Launching a use case from C-01-03
2. Receiving a scan of a document and opening a search form and verifying the identity of the signature, seal and stamp
3. Selecting a verification method (automatic, using a filter by organizations and officials)
4. Entering parameters for a query in the database
5. Formation of a query in the database for comparison
6. Receiving a response from the database and displaying it on the screen
7. Allowing the user to confirm the comparison
8. Completion of the use case.

Use case execution time: the execution time of this use case is not regulated by the System, it depends on the user's actions. The execution time of a query in the database is regulated by the requirements described in section 4.1.4. of this ToR.

Input data: Scanned document (signature, seal, stamp data).

Output data: The result of the comparison.

Apostille authentication

Use case number: *C-01-05*

Launch conditions: Check Apostille functionality

Process owner: *User (any role)*

Use case execution order:

1. Launching the Check Apostille functionality
2. Using a verification link or QR code
3. Sending a request to E-register to receive apostille data
4. Returning a response from E-register and displaying the results to the user
5. Completion of the use case

Use case execution time: the execution time of this scenario is governed by the requirements described in section 4.1.4. of this ToR.

Input data: *link for apostille authentication.*

Output data: *a list of apostille parameters (or a message about the absence of data)*.

Adding Scanned Documents

Scenario number: C-01-06

Start conditions: Execution of scenario C-01-01, step of adding scanned documents

Process owner: System process

Script execution order:

1. Referring to the script;
2. Opening the form for adding documents;
3. Selecting document (s) on the local disk of the user device;
4. Checking the correctness of the format of the added documents;
5. Checking the quality of the added documents;

6. Sending a request to the server to save the added files;

7. Completion of the script.

Script execution time: The execution time of this script is governed by the requirements described in section 4.1.4. of this ToR.

Input data: documents added by the user.

Output data: scanned versions of documents saved in the system.

Possible expansion of the scenario: possible expansion of the number of accepted formats of scanned documents and their verification.

User authorization in the system via One-ID

Scenario number: C-01-07

Launch conditions: Launch of the authorization functionality by the user

Process owner: User (individual)

Script execution order:

1. Launching the system

2. Selecting the form of authorization of the One-ID platform

3. Entering authorization parameters (series and number of the passport, PINFL)

4. Sending parameters for verification on the One-ID platform

5. Returning a response from the One-ID platform

6. In case of a negative answer, go to item 9

7. Creation of a user session

8. Providing the user with access to the Personal Cabinet

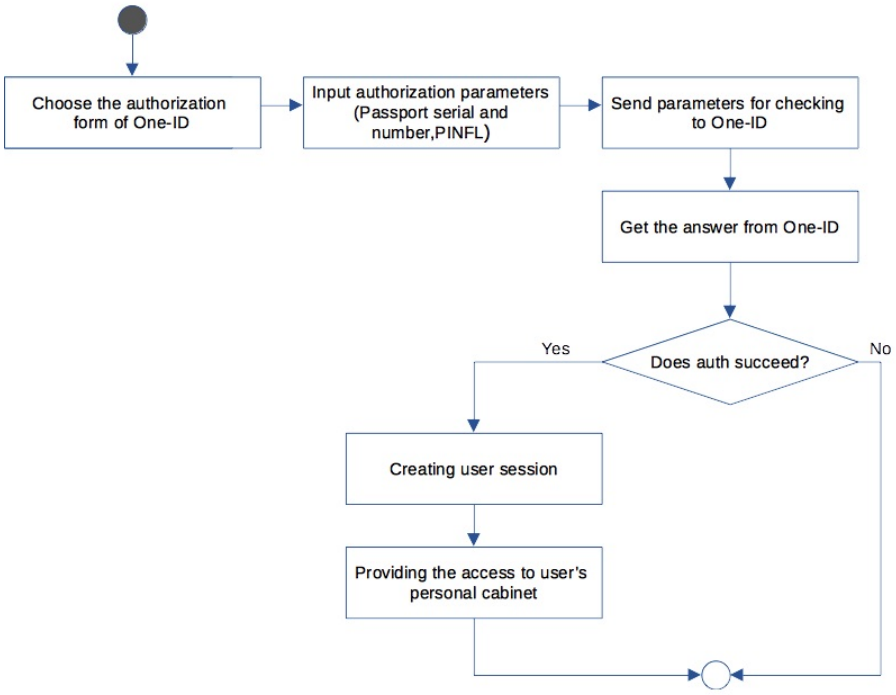
9. Complete the script.

Script execution time: the execution time of this script is not regulated by the System, it depends on the actions of users.

Input data: Passport series and number, PINFL.

Output data: User session identifier.

Scenario outline:



User authorization using digital signature

Scenario number: C-01-08

Start conditions: System start, authorization selection

Process owner: User (legal entity or individual), employee of the approving agency

Script execution order:

1. The user opens the authorization and registration page and selects the type of authorization with EDS.
2. Redirect to id.egov.uz page.
3. EDS selection and password entry
4. Confirmation of data by the ESI system
5. Receiving a response from the ESI about successful authorization.
6. Granting the user access to the system (creating a user session).
7. Completion of the script.

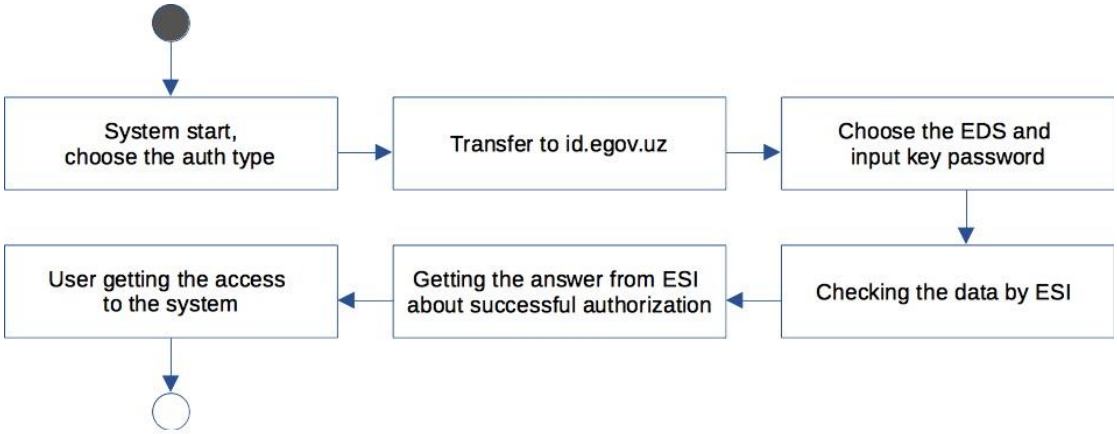
Scenario execution time: the time schedule for the script processing is regulated by the response time of the external system (ESI).

Input data: Electronic key (when using EDS).

Output data: user session identifier.

Scenario C-01-08 is not intended to be extended and is only aimed at providing users with access to IP, including access by legal entities and employees of responsible approving authorities.

Scenario outline:



Checking the status of the application

Scenario number: C-01-09

Launch conditions: Launching the section of sent orders, requesting the status of the selected order

Process owner: User (legal entity or individual)

Script execution order:

1. The user opens a page with a list of applications sent for consideration.

2. Selects an application for requesting status on it.

3. The system sends a request to the server to receive information about the details of the application (including status)

4. Receiving a response from the server and generating a page for details of the application for the user.

5. Completion of the script.

Execution time of the script: the total execution time of the script is not regulated and depends on the actions of the user in the system; the execution time of the request to the server is regulated by the requirements described in Section 4.1.4. of this ToR.

Input data: Electronic key (when using EDS).

Output data: user session identifier.

Note: the status of the application can also be requested when forming the page for the list

of sent applications and displayed directly in the list.

Unloading apostille documents from the system

Scenario number: C-01-10

Launch conditions: launching the functionality of unloading apostille documents

Process owner: User (legal entity or individual)

Script execution order:

1. For documents in the "Ready" status, the document uploading functionality is initiated.

2. Sending a request to the server to issue a document.

3. Receiving a response from the server and opening a pdf document in a new browser tab (displaying pdf format implies the possibility of uploading and printing a document).

4. Completion of the script.

Script execution time: the execution time of a request to the server is governed by the requirements described in section 4.1.4. of this ToR.

Input data: ID of the application, as well as the document.

Imprint: apostille document in pdf format.

Formation of statistical reports

Scenario number: C-01-11

Launch conditions: Launch of the statistics generation functionality

Process owner: user (administrator, department employee)

Script execution order:

1. Launching the statistics functionality;

2. Selection of statistical sample parameters (see p.4.2.6.7);

3. Sending a request to the server to generate statistical data;

4. Obtaining statistical information from the server and generating it for viewing by the user.

5. Completion of the script.

Script execution time: the execution time of a request to the server is governed by the requirements described in section 4.1.4. of this ToR.

Input data: request parameters.

Output data: statistical sample corresponding to the parameters of the request.

Possible scenario extensions: the number of parameters for statistical sampling can increase over time in accordance with the requirements of the Customer.

Apostille signing with EDS

Scenario number: C-01-12

Launch conditions: Launch of the apostille affixing functionality

Process Owner: Approving Authority Officer

Script execution order:

1. The user activates the functionality of affixing an apostille.

2. Redirected to Unicon Key Registration Center page.

3. EDS selection (in the EDS module of the integrated system);

4. Adding an EDS to the document;

5. Receiving a response from the Key Registration Center about successful authorization.

6. EDS affixing on the document to be apostilled.

7. Completion of the script.

Scenario execution time: the time schedule for scenario processing is regulated by the response time of the EDS module.

Input data: Data for obtaining an EDS.

Imprint: EDS and generated apostille.

Scenario C-01-12 does not imply any extension and is aimed only at ensuring the identification of users for affixing an EDS to a document.

Administrator authorization in the system

Scenario number: C-01-13

Launch conditions: Launch of the authorization functionality by the administrator

Process owner: administrator

Script execution order:

1. System startup

2. Entering authorization parameters (login and password)

3. Sending parameters for verification to the server

4. Returning a response from the server

5. In case of a negative answer, go to item 8

6. Creation of a user session

7. Providing the administrator with access to the system

8. Complete the script.

Script execution time: the execution time of this script is not regulated by the System, depends on the administrator's actions.

Input data: login and password.

Output data: User session identifier.

4.1.1.4. IS Diagnostics Requirements

To ensure high reliability of the functioning of the IS and its individual components, the requirements for diagnosing its state must be met.

Diagnostics of the IS should be carried out using standard tools included in the software package (on the backend side).

It is compulsory to keep logs of incidents in electronic form, as well as schedules and logs of scheduled preventive maintenance. All technical components of the back end must be monitored regularly and continuously.

For technical components, it is necessary to provide diagnostics in accordance with the recommendations of the equipment supplier.

4.1.1.5. Prospects for the development, modernization of the IS

The main principle in the development of IS is the principle of scalability of the software part, so that the system can develop and grow with additional modules that perform new functions, on demand and in accordance with the conditions of the Customer.

4.1.2.Requirements for interaction with third-party information systems

Interfaces (API) must be developed in accordance with the requirements of the state standard O'z DSt 2590: 2012, to integrate IS with third-party systems, with other state ISS

To receive data from third-party information systems in the IS, APIs will also be generated and sent to the backend for further processing.

The IS must use APIs developed under the Technological Instructions approved with the integrated offices. Technological instructions should be drawn up with the assistance of the Contractor. The customer is responsible for the approval of the Technological instructions with external organizations.

API interaction must be authorized, all API functional methods must be called after the authorization procedure. All API calls must be logged at the IS database level.

It is necessary to support the JSON, XML, WSDL formats as the format of the transmitted and received data in the IS.

The interaction of the System with third-party ISs must be carried out via the HTTPS data transmission and reception protocol.

The IS should use unified reference books and classifiers adopted in the Republic of Uzbekistan "Clissifiers.gov.uz" (hereinafter with the new version of cs.gov.uz).

4.1.3.Requirements for the number and qualifications of users

The IS is intended for use among a wide range of users, therefore the maximum number of end users who simultaneously have access to the IS is limited only by the technical limitations of the server part of the System.

The solution should provide the ability to quickly and simultaneously access a large number of users to the IS database to provide services, change and analyze the necessary information, and process requests in real time.

The user interface should only display those tools, functions, and methods that might be required by a user with that particular level of access.

The following roles should be envisaged in the work of IS:

№	User groups
1	Applicant - a user who wants to receive the service of affixing an electronic apostille through the Single Portal
2	Responsible employee - a user working in the relevant ministry or department, accepting applications, as well as verifying documents and signing an apostille
3	PSA employee - a user participating in the processes of accepting applications, monitoring and controlling the issuance of apostilles
4	Administrator - a user who has full access to system settings, directories, user accounts, event logs and other system data.
5	Guest - a user who wants to verify the authenticity of the apostille using the QR code.

Provide a minimum level of qualification requirements that users need to work in the System (minimum level of computer education). Requirements for the role PSA employee - an average level of computer education, for the role of Administrator - a high level of computer education.

4.1.3.1. Requirements for professional education, competencies and skills of personnel

The number of personnel on the part of the Customer should be sufficient for information and technical support of the IS in the absence of unexpected hardware failures and force majeure circumstances. The minimum requirements for professional education, competencies and skills of personnel are determined by job descriptions and taking into account the proposals of the Developer.

The proposed list of personnel categories and the required qualifications are presented in the table below.

Personnel category	Personnel qualifications	The order of preparation and control of knowledge and skills
Maintenance personnel	1) Skills of maintenance of software products and hardware of server and communication equipment 2) Skills in diagnostics of computer hardware failures	Special education, specialized courses in software maintenance, administration of server and communication equipment.
Support group	1) Professional knowledge of the operating systems, database management systems and methods of their system administration 2) Knowledge of networking and telecommunications technologies 3) Knowledge of information security technologies	Special education. Control: interview, certification documents, trial work, trial period.

4.1.3.2. Requirements for the mode of work of personnel

There are no special requirements for the mode of operation of IS users.

4.1.4. Destination indicators

The IS should provide the ability for at least 5,000 users to work simultaneously with the following response time characteristics:

- for navigation operations on screen forms without accessing the database - no more than 1 sec
- for operations related to queries in the database - no more than 10 seconds (depending

on the network speed)

- for operations related to interaction with external systems - no more than 10 seconds (depending on the network speed)
- for other operations - no more than 5 seconds.

4.1.5.Reliability requirements

The IS should maintain its operability and ensure the restoration of its functions in the event of the following emergency situations:

- in case of failures in the hardware or software part of the user's terminal device (workstation), leading to a reboot of the operating system, the program must be restored after the device is rebooted
- in case of errors in the work of workstations, the restoration of the IS function is assigned to the operating system of the device
- in case of errors related to the software of the workstation, the restoration of operability is assigned to the operating system

The hardware part must be built in accordance with the requirements of the State standard O'z DSt 2875: 2014 “Requirements for data centers. Infrastructure and information security”, including redundancy and the absence of a single point of failure of hardware. A solution with load balancing across hardware nodes should also be applied, including server capacities and data storage.

All IS databases should be backed up to an external server with a frequency of 1 time per day. Backups must be kept for at least 3 months. Moreover, the hardware must be implemented with active / standby redundancy in order to ensure the transfer of the load to the backup server in case the active one is out of order for any reason. The data on the active and standby nodes must be fully synchronized.

The IS should exclude accidental calls of procedures, functions, commands used in the functionality. All calls to functions, methods, procedures must be carefully checked for accidental calls.

The IS should be protected against misuse of functions by users.

The IS should ensure correct handling of situations caused by invalid and inconsistent input data values. In these cases, the IS must issue the user with appropriate alarm messages, and then return to the operating state that preceded the incorrect (invalid) command or incorrect data input.

The IS, after carrying out work on this Terms of Reference, must be resistant to software and

hardware errors, with the ability to restore its operability and the integrity of information content in the event of errors and failures of user workstations.

The IS should support up to 10 million users by the third year of operation, 1 million active users.

4.1.6.Safety requirements

The IS must comply with the general requirements for the security of software when operating as part of information systems.

The principles of building a solution must meet modern international standards in terms of the degree of security and safety of information and include:

- means of encrypting information sent by users
- methods to protect the database from unauthorized access
- logging and audit, registration of all events and user actions
- restriction of user access to IS objects based on user identification, including by his role
- access to data is limited by access rights, which are determined by the roles of IS users: the user interface displays only those tools, functions and methods that can be requested by a user with a given specific level of access
- flexible management of access rights; enabling the Administrator to maintain user accounts
- protection of data transmission channels
- differentiation of access rights of users and IS Administrators will be based on the principle "what is not allowed is prohibited"
- protection of transmitted information by encrypting confidential data during transmission over communication channels

The technologies used in the development should ensure the security of access to data through authentication, identification and role-based user rights.

When the system operates at the IS backend level, logging of each user session should be implemented, indicating the MAC address of the device from which the system was logged in, and the time of logging into the system.

Automatic audit logging should also provide the ability to monitor the most critical (unique) data stored in the database and record all events that occur and any changes in any data in the

system in accordance with the system configuration.

The audit trail should be generated automatically and maintained continuously. Each operation in the audit trail must be identified by user, date and time. The audit trail should be protected from revision and deletion of records.

Since the IS will work in conjunction with the Web server, all requests must be transmitted over secure connections based on the set of SSL / TLS protocols of the latest possible versions over an encrypted HTTPS channel using an SSL certificate, this will maintain a stable speed and a high degree of security between the application and the Web. -server.

The customer must ensure that the server rooms and the conditions for their equipment and equipment meet the necessary requirements for the normal functioning of the System, as well as compliance with the requirements of the State standard O'z DSt 2875: 2014 “Requirements for data centers. Infrastructure and information security”.

All external elements of the technical means of the information system, which are energized, must be protected from accidental contact, and the technical means themselves must have a protective earthing.

The power supply system must provide protective shutdown in case of overloads and short circuits in the load circuits, as well as emergency manual shutdown.

Installation and commissioning of the system, as well as its subsequent maintenance should not be associated with exposure of personnel to dangerous values of electric current, electromagnetic fields, acoustic noise, vibrations, etc.

4.1.6.1. Requirements for protecting information from unauthorized access

The IS must comply with all the established requirements in the current normative documentation of the Customer for the protection of information from unauthorized access.

The IS should ensure the limitation of physical access to the elements of the system, both in order to prevent disruption of the system, and in order to obtain unauthorized access to information.

The IS should implement a mechanism for the security and protection of information based on the following basic principles:

- limiting access to the system based on user identification
- restricting access to system objects

- audit logging to identify unauthorized changes to the system
- protection of data transmission channels.

The IS should provide the function of controlling access to the information resources of the Portal.

During development, the list of personalized data can be expanded.

The IS should ensure the provision of information for maintaining logs (Logs), which record information about system events, attempts to unauthorized access to information for all IS users.

Information protection should include a set of organizational measures and hardware and software methods and information security tools to prevent unauthorized access to information resources. The IS should ensure the integrity, availability and confidentiality of data during their processing.

When developing the IS, the requirements of the information security policy in force for the Customer must be taken into account in order to avoid the occurrence of conflict situations when carrying out measures to ensure information security.

User passwords must meet password complexity requirements to prevent brute-force attacks. The number of unsuccessful attempts to enter the IS should be limited and when it is exceeded, the IS should be blocked for a certain period of time. No one should have the right to modify / delete log entries.

4.1.6.2. Requirements for the safety of information in case of accidents

Information security at the IS software level should be ensured when:

- emergency situations in the premises where the IS servers are located
- network failures caused by loss of power
- technical failures.

In case of disasters, the system has the ability to fully restore data through backup. At the software level, it is necessary to prevent partial or complete loss of user data and violation of the integrity of the information stored in the database.

At the level of technical means, the system must have built-in tools for diagnosing information integrity violations. In the event of a system failure, the administrator should be able to view, at the level of logs and other system logs, the probable data corruption in the event of a failure and take the necessary measures to recover the data.

The system must provide backups of its own database as well as the system settings to be used to restore the system. Backups should be stored on non-volatile media and periodically updated as new data becomes available and / or at least once a day. Data recovery should be done by selecting the last uncorrupted copy.

Restoration of a backup copy of data from an external medium should be carried out by means of a DBMS with the participation of an administrator. The hardware part should be implemented taking into account active / standby redundancy to ensure the transfer of the load to the backup server in case the active one is out of order for any reason. Data integrity control between the active and standby servers should be carried out in real time.

The technical means of the system must be equipped with uninterruptible power supplies (UPS) to protect against voltage surges and unexpected power outages.

Information security must comply with the requirements established in the current editions of standards: O'z DSt ISO / IEC 13335-1, O'z DSt ISO / IEC 15408-1, O'z DSt ISO / IEC 15408-2, O'z DSt ISO / IEC 15408-3, O'z DSt ISO / IEC 27001, O'z DSt ISO / IEC 27002, O'z DSt 2814.

The information displayed in the IS should not lose its quality (relevance, completeness, reliability), be destroyed, damaged, distorted and lost in the event of any emergency situations: failure of technical means, loss of power in the power grid, etc.

4.1.6.3. Requirements for protection against the influence of external influences

It is necessary to use shielded cables, shielding the premises where the equipment should be located, to take into account the conditions for the joint use of radio electronic means (radio communications, television and radio broadcasting transmitters, cellular and paging communication systems, etc.) in which mutual interference does not affect the performance of the equipment.

The equipment intended for the operation of the IS must be resistant to external influences.

The equipment intended for the operation of the IS, in packed form, must withstand storage for a year (including transportation) in warehouses at temperatures from -50 ° C to +40 ° C, with an average monthly value of 80% relative humidity at a temperature of +20 C (allowed short-term increase in humidity up to 98% no more than 1 month per year).

In case of loss of performance in case of failures, errors or failures of software and hardware, the IS must provide a 100% guarantee of the safety of information.

The rules of the IS should provide for the creation of backup copies of databases and related information.

4.1.7. Ergonomic and technical aesthetics requirements

The IS should provide user-friendly interfaces that meet the following requirements:

- When creating an IS, a convenient and intuitive interface should be developed for a user who knows his subject area well and is not a specialist in the field of information technology.
- User interfaces of the IS should be designed and developed using uniform principles of graphical presentation of information and organization of access to functionality and services.
- A graphic design of user interfaces, color, font and compositional solutions for displaying texts, images, tables, hyperlinks, controls and navigation elements (menus, buttons, forms, etc.) should be developed, fields for filling should have notes about the data, to be entered.
- The IS should ensure high-quality interaction of the user (person) with the system.
- The main requirement for ergonomics and technical aesthetics is the adequacy of the response time of the IS components to the complexity of the user's request to the databases:
    - when performing standard requests, the user must work with the IS in real time (up to 1 second per response)
    - the user must receive a response from the system within 5 seconds after sending standard requests (with the best possible network signal quality)
    - when executing complex queries that require a long time to execute, the user should receive a warning about the waiting process
- The design of the components of the presentation level of the IS should be developed taking into account the standard ergonomic requirements for the user graphical interface, which ensures the comfort and productivity of its users, as well as fast loading of the pages selected by the user.
- When developing an interface design, the convenience and ease of understanding of the interface should be prioritized. The design of user interface elements should evoke a minimal understanding of the actions that the user will take when interacting with one of the elements. Interface elements should not be associated with functions that they

do not perform. Design solutions must comply with applicable sanitary and ergonomic standards and most effectively create a positive emotional response among IS users.

- The system's user interface design should be responsive to most screen resolutions.

The following minimum list of requirements must be applied:

- The IS should have a convenient navigation system, that is, the ability to navigate to the information of interest in 1-3 clicks.
- All information should be divided into blocks and highlighted with design details for the convenience of working with it.
- The structure of the IS should be designed in such a way that, being on any page, the user understands where he is and how to navigate to the information of interest.
- Navigation is carried out using links to the type of information display in the IS, as well as links to data objects.
- Interface elements should not be associated with functions that they do not perform.
- The design development should take into account the most modern design solutions UI (user interface) and UX (user experience) for the convenience of users.

4.1.8. Portability requirements

No portability requirements.

4.1.9. Requirements for the operation, maintenance, repair and storage of IS components

Minimum IS lifecycle:

- in general - at least 10 years
- individual functional modules - at least 3 years;

Requirements for the IS lifecycle at the stages of industrial operation should be clarified during the development process.

Periodic maintenance of the used technical means must be carried out in accordance with the requirements of the technical documentation of the equipment manufacturer.

The operation of technical means of information technology and the security of the premises in which they are located must be ensured in compliance with the requirements of the guidance

document RH 45-201: 2011 “Technical requirements for buildings and structures for the installation of computer equipment” and the state standard 0'z DSt 2875: 2014 “Requirements for data centers. Infrastructure and information security”.

The system should allow the administrator to monitor the state of the system according to the following indicators:

- Monitoring the operation of services and applications as part of the system
- Monitoring the operation of the system interfaces
- Monitoring the functioning of the database
- Control over the operation of the technical means of the system.

The administrator must be able to gain remote access to the system, including to monitor the health. Remote access should be provided over secure communication channels.

4.1.10. Requirements for patent and license purity

The Contractor must use only intellectual property objects, the rights to which are acquired (received) and used without infringement of intellectual property rights of third parties or provided by the Customer. This requirement must ensure that the copyright, related, patent and other rights of the developers of the third-party components used are respected.

The Contractor undertakes to transfer, free of charge to, the rights to use the protected results of intellectual activity, the rights that belong to the Contractor and (or) third parties, and which were used by the Contractor.

4.1.11. Requirements for standardization and unification

At all stages of project development, the unification of design solutions should be ensured, which should be ensured by a uniform approach to solving similar problems, unification of technical, informational, linguistic, mathematical, informational and organizational support. A uniform approach to solving similar problems should be achieved:

- unification of the functional structure in terms of the implementation of automated functions and information links between them
- the same software and hardware method for implementing such system functions and a single interface with the user that meets international standards.

The unification of technical means should be achieved through:

- the use of serial technical means that meet international standards

- minimization of the types of computers and other components used
- use of standard automated workstations, components and complexes

Unification of information support should be achieved through:

- using a unified system of classification and coding of objects and sub-systems
- the use of national, industry and other standard classifiers used in the practice of the functioning of the facility
- use of standard forms of documents (reports) and rational limitation of their composition types (as agreed with the Customer)
- application of uniform methods and means of collection, preparation, control and storage of information arrays of the system.

The unification of software should be achieved due to the modular principle of constructing algorithms and typing algorithmic modules.

Software unification must be achieved through:

- maximum possible use of standard software
- the use of unified software modules in the development of application programs.

Indicators that establish the required degree of use of standard, unified methods for implementing the functions of the System, supplied software, typical mathematical methods and models, typical design solutions:

- support for modern transport protocols: TCP / IP, HTTP (S);
- support for Internet standards: RESTfulAPI
- support for search engine implementation standards
- support for the most common document formats: Json, Json-rpc, XML, HTML, Javascript
- support for cluster solutions with load balancing
- support for distributed information retrieval
- support for distributed access to information
- the ability to operate on various hardware platforms

The coding and classification system used to generate reference information must meet the requirements for the classification and attribution of documents adopted in the territory of the Republic of Uzbekistan, as well as take into account the world experience in creating such systems.

The solution being developed should ensure the unification of functional tasks, operations

and user interfaces.

4.2. Requirements for the functions (tasks) performed by the IS

4.2.1.User authorization module

The user authorization module is designed to provide applicants with access to the system functionality (Scenarios of use C-01-07, C-01-08) ..

The IS must allow authorization by means of One-ID, as well as using EDS. Legal entities will be able to log in using EDS.

Authorization must be available through the Single Portal.

4.2.2.Authorization module for departments

One of five responsible departments can participate in the apostille affixing:

- Supreme Court;
- Ministry of Foreign Affairs;
- Inspectorate for Quality Control of Education;
- Territorial administrations of justice;
- General Prosecutor's Office.

An account must be created for each responsible employee in the system. Authorization must be done using an EDS when interacting with the ESI, according to the electronic keys of the internal module of the system

Also, access to the IS should be organized for employees of the Public Services Agency in order to use the functions of sending applications, monitoring the processing of requests for apostille and monitoring the system's performance.

4.2.3. Administrator authorization module

The administrator authorization module implies the Administrator's access to the system using a dedicated administrator login and password (Scenario C-01-13). Changing administrator credentials is possible only by the administrator himself or through the system tools available during development.

An administrator can create additional accounts for the Administrator role with similar rights.

4.2.4.Storage module for signatures and seals

The system should allow storing and using digital and graphic signatures (signatures and seals), keeping records of them, and allowing control over the terms of their use in accordance with

the regulations.

This module should allow carrying out a graphical analysis of the compliance of the signature of the documents (scans) to be apostilled and the seals of the organizations that issued them. (Scenario C-01-04).

When generating signatures, the following information about the official is required:

- Full name
- Position
- Office
- Email
- Comment
- Is the account active
- From which to what date is the account active
- Photo signature
- Photo of the seal and stamp in good quality

For the functioning of this module, samples of all signatures and seals, stamps of the responsible authorities will be collected, the documents of which are submitted for consideration and obtain an apostille.

4.2.5.User account

In the user's account, the applicant gets the opportunity to work with electronic apostilles, including:

- Formation of an application for obtaining an apostille (Scenario C-01-01)
- Adding scanned versions of documents for review (Scenario C-01-06)
- Checking the status of applications (Scenario C-01-09)
- Unloading of the finished apostille document (Сценарий C-01-10)

4.2.5.1. Application generation module

Formation of an application for an Apostille (one document or a package of documents) is carried out by the applicant.

In this module, data must be filled in (not limited to):

- Individuals’ personal data, full name:

        - Passport series and number;
        - PINI;
        - Date of Birth;
        - Address;
        - Phone number;
        - Email address;
- Legal entity data (Name of legal entity):
        - TIN of the organization;
        - Name of company;
        - Legal address of the organization;
        - Email address;
- Number of apostilled documents;
- Type of documents to be apostilled (there must be a single type for one case);
- Scan of the apostilled document (each);
- Date of filling in the application (generated automatically).
    - Details of the document to be apostilled (date, number, city);
    - Departure country;
    - Filling language (eng / uzb).

When choosing the type of the first document to be submitted, the user should see the entire list of submitted documents. When adding the following documents, the list of document types should be sorted according to the office of destination. This paragraph will allow to exclude the addition of documents related to different offices to the application for consideration.

When filling out the application, provide a field that determines in what form the apostille will be issued, in paper or electronic. At the first stage of the implementation of the system, it is necessary to use any of the options (paper or electronic) both when submitting an application and when receiving an apostille.

Note: Several documents can be submitted in one application, but all of them must be sent to only one office. In this case, payment is made for the submission of one application. In the event of a possible error, when the document gets to another office not for its intended purpose, it is necessary to provide in the system with the possibility of redirecting the application to another office without returning the application to the applicant. Employees of the PSA or the responsible

authorities should consider the application and correctly forward the request.

4.2.5.2. Module for adding scanned versions of documents

In this module, the user adds scanned documents in .pdf format to the system. The system should automatically check the quality of the added document and, if it is impossible to recognize the document, issue an error.

All scanned versions of documents can be added from the local disk of the user's personal computer to the document storage of the user's personal account. Further, documents from the repository can be attached to the application.

It is also possible to attach a document from a local disk directly to the application and automatically save the document to the storage.

4.2.5.3. Application status check module

The user should be able to see a list of his submitted applications for obtaining an apostille and see the statuses for each application.

If the user has sent several documents related to different departments to obtain an apostille, then each of the documents can have its own status, while the general status of the application is formed from the status of the most belated document. In the case of a partial positive review (some of the documents are apostilled, and the rest are not affixed), then the user will see the review statuses directly on the documents.

Possible application statuses for the user:

- Under consideration
- Reviewed
- Refused

Possible statuses of documents included in the application:

- Under consideration
- Done
- Refused

Allow the user to view any of the requests sent to them. Among other things, it is necessary to create sorting by documents for which an apostille has been received.

The user should be able to receive notifications regarding changes in the status of applications or documents in applications.

4.2.5.4. Apostille download module

The user must be able to:

- Download the Apostille and printing it in .pdf format.
- View the history of applications and results of consideration (using filters by date, type of document, result of consideration of each document, etc.).

The apostille document is generated according to the approved template.

Apostille parameters:

1. Full name of the official who signed the official document submitted for apostille

The official name of the government agency that issued the official document.

When the apostille is affixed on a notarized copy of an official document, the words "notarized copy" after the words "this public document" in line 1 of the apostille, as well as the name and position of the notary and the name of the notary office, respectively.

2. The position of the person who signed the official document. If the official document is signed by more than one person, the highest position in their position is indicated (for example, the presiding judge)
3. The official name of the organization that issued the official document
4. The city, the country in which the apostille was affixed
5. Date of apostille affixing in numbers
6. Full name and the position of the person who apostilled the official document
7. The sequence number corresponding to the sequence number in the E-register
8. Type of apostille issued (in electronic or paper form)
9. Apostille QR code (unique on a global scale)
10. symbol / seal of the issuing state authority
11. information about the electronic signature

At the bottom of the document on each apostille, there must be a postscript that this document can be verified at the indicated (designated) web address.

4.2.6. Department's account

The account of the department is intended for receiving applications directly related to this department, reviewing documents, entering additional information into the system, signing an apostille or refusing to issue an apostille for this document (Scenario C-01-03).

Each department must receive applications in accordance with the rules of examination.

4.2.6.1. Document queue module

The module assumes working with a queue of documents (applications) for consideration to obtain an Apostille (The function is an extension of the scenario C-01-03).

The module implies the use of the possibility of editing an application, checking the attesting signature in the signature and seals module, attesting, changing the status.

The parameters of each order are similar to those described in section 4.2.4.1. of this ToR.

4.2.6.2. Dossier Module

The Dossier module should provide an opportunity to view the Dossier of all considered documents / applications, regardless of whether the document was apostilled or not (The function is an extension of the scenario C-01-03).

4.2.6.3. Stock module

The module should be able to view rejected applications. When reviewing documents, it must be possible for the responsible officer to make a comment based on the results of the review. This comment is required for internal use only (The function is an extension of the scenario C-01-03).

4.2.6.4. Signed documents module

The module assumes working with signed documents, including viewing and searching through them. (The function is an extension of the scenario C-01-03). It should also be able to view all scanned versions of documents.

The search should be organized in accordance with the requirements of section 4.2.5.5. of this ToR.

Apostille parameters are described in section 4.2.4.4. of this ToR.

4.2.6.5. Search module

The IS should provide employees of departments with an advanced search function for all documents / application in the database (The function is an extension of the scenario C-01-03).

Advanced search for documents should include, among other things, filtering parameters for documents by type, by approving employees, by territorial affiliation, by the date of the Apostille affixing, by the applicant's surname and other possible parameters.

4.2.6.6. Module for monitoring the provision of public services

This module allows the PSA employees to monitor the provision of public services, in particular, to control the deadlines for the execution of applications, to transfer erroneously transmitted applications to their destination. (The function is an extension of the scenario C-01-03).

A PSA employee, at any time, must have access to following information:

- A complete list of pending applications
- List of applications with an expiring consideration period (for generating notifications)
- Applications transferred to the PSA for transfer to another department by appointment
- The applications on which the decision was made for the selected period
- Applications for which the Apostille has not been issued (refusals)
- Office-specific applications
- Applications related to a certain official who affixes the Apostille

At the development stage, other parameters may be provided for control by the PSA.

4.2.6.7. Statistics module

The IS should provide for the formation of statistical data on the volume of applications, issued Apostilles, as well as in the context of departments, countries / regions / districts, individuals / legal entities, etc. (Scenario C-01-11)

A complete list of statistical parameters for the sample will be determined at the stage of system development.

4.2.7.Administrative module

The implementation of the administrative module is not considered in the scenarios for the use of IS, and can be proposed by the Contractor, based on the best practices in the implementation of information systems projects.

The administrative module is intended mainly for the employees of the Public Services Agency, who will carry out the functions of monitoring the health of the system, generating a signature sheet, and should also be available to them:

- Dashboard for all main indicators of Apostille issuance

- A list of incoming applications and the possibility of sending applications in accordance with the regulations to the responsible departments (in case there was no automatic distribution)
- A dossier sheet for pending applications
- Viewing statistics on various indicators (Scenario C-01-11)
- Functional formation of a register / database of signatures, seals and stamps of officials who can sign official documents for their further identification with signatures, seals and stamps on the submitted document with signatures, seals and stamps contained in the IS database
- Rejected cases list (stock)
- Advanced search functionality (similar to that described in section 4.2.5.5 of this ToR);
- Section for the formation of accesses (roles and accesses for users - employees of departments)
- Section for viewing system logs
- Section for managing directories and classifiers.
- Part of the functionality repeats the functions described in section 4.2.6 of this Terms of Reference.

4.2.7.1. Managing user roles

In this module, the administrator has access to all user accounts with the ability to sort by role.

The administrator must have access to lock the user account, and create accounts, including sending credentials to users, change the roles of user accounts.

4.2.7.2. Formation of an access matrix

The administrator must have access to the functionality of access control in relation to user roles.

Access should be formed in relation to functional elements and sections of both the user interface and the administrative module.

Regulation of the access table should allow the creation of new user roles without violating the logic of the functioning of the IS.

4.2.7.3. Managing directories and classifiers

System module, which is designed to generate reference data for the operation of the IS. In the form of directories, all auxiliary data for filling out the lists can be drawn up. Reference books and classifiers should be available in the administration module. For general reference books (widely used data), it is planned to integrate with the "Register of Reference Books and Classifiers" "clissifiers.gov.uz" (hereinafter with the new version of cs.gov.uz) to ensure the use of unified reference books and classifiers of the Republic of Uzbekistan.

4.2.7.4. Viewing logs

The IS should keep logs of all system events, including:

- events for all intersystem interactions
- all user actions in the IS

When viewing the logs, it should be possible to sort the information by date, username, event type and other possible parameters for the convenience of finding the desired event. This functionality must be available to the System Administrator.

4.2.7.5. Service monitoring

Service monitoring should allow the system administrator to control the performance of all software modules and IS interfaces, as well as use a minimum test set of tools for verification.

4.2.7.6. "Help" Module

The module is designed to accommodate tips and help sections when working with the system. The user must at any time be able to receive comprehensive information about what data to enter, what requirements are imposed on the entered data, what regulations for affixing an apostille, and more.

4.2.7.7. Notification module

All basic types of notifications to users are generated in the notification module.

For applicants:

- Change in the status of the application / document in the process of consideration
- Completion of consideration of the application

For departments/agencies:

- Receipt of applications
- As the signature is about to expire

4.2.8.Apostille information request module

The module is intended for access by external partners, interested parties to check the status of the Apostille (relevance and authenticity) and the main details of the issued Apostille, as well as scanned versions of documents (Scenario C-01-05).

An organization or any interested user, both in the Republic of Uzbekistan and abroad, who wants to check the Apostille by QR code, sends the request through a special form Apostille check. The request is sent to #E-register", from where the response is returned. When checking by QR code, all information, and details of the requested Apostille must be provided. The module should also allow checking the Apostille by the entered number and date of issue.

Apostille parameters required for display during authentication are given in section 4.2.4.4. of this Technical Assignment.

4.2.9.Integration module

The module provides for the organization of interaction with external systems in accordance with the approved technological instructions. (see section 4.1.2 of this ToR)

Provide for the possibility of expanding the system in the future to interact with other information systems in terms of receiving / exchanging information.

The first stage implies integration with Single Portal for authorization in the system through the Single Portal, as well as the ability to download and view ready-made apostilled documents in the Single Portal.

Integration with external systems implies the receipt of personal data of legal entities and individuals. The first stage implies integration with the Single Portal, SPC (DI, DL, obtaining personal data), the Ministry of Internal Affairs (data on registration of individuals), State Tax Committee (receiving data from legal entities), with an SMS gateway for sending notifications to users, and payment systems.

Integration with the EDS Key Registration Center (Unicon) is also provided. This type of integration for obtaining an EDS and verifying its authenticity is necessary for affixing the apostille directly. It is mandatory to implement an EDS for affixing an apostille in accordance with the international standard.

Integration by the Register of directories and classifiers "clissifiers.gov.uz" (further with the new version of cs.gov.uz) should be organized. IS should use unified reference books and classifiers

adopted in the Republic of Uzbekistan.

4.2.10. Payment processing module

To apply for the service of affixing an electronic apostille, the user must pay a state fee for consideration. To do this, it is necessary to organize integration with payment services so that the user can pay for the application online. (Scenario C-01-02).

The cost of the application is formed based on the tariff for the review service. An application can include several documents sent to one office.

The IS should interact with payment systems and receive information from them for internal billing.

Billing should compare the payments made with the accounts for which they were made, as well as the applications for which payments were made, fix the payment dates and issue data upon request for the user's personal account and regulatory agencies.

Integration with payment systems is carried out according to agreed technological instructions and dedicated API.

It is expected to receive the following data:

- payment date
- Account for payment
- Paid amount

Payment data analytics should be performed on the IS side in the payment module.

4.2.1. E-register backend

In the backend, all system processing is carried out, including calls to the database, the formation of requests and the processing of responses sent and received via the API in all directions.

Processing scenarios implemented in the IS backend can be proposed by the Contractor, based on the best practices in the implementation of information systems projects

4.3. Requirements for types of support

4.3.1.Requirements for software

The description and content of algorithms executed in the IS is determined in the process of software development.

4.3.2.Information support requirements

The composition, structure, and methods of organizing data in the System should be determined at the stage of detailed design. The database model must be submitted for approval to

the Customer by the Contractor at the stage of detailed design.

Information exchange of data in the system should be carried out using the developed communication protocol for data transmission. Data storage in the system should be built based on modern DBMS.

To ensure data integrity, the built-in mechanisms of the DBMS should be used. The means of the DBMS, as well as the means of the operating systems used, must provide documentation and logging of the information processed in the system. The structure of the database must support the encoding of the stored and processed information. Access to data should be provided only to authorized users, considering their official authority, as well as taking into account the category of the requested information.

The DBMS tools, as well as the tools of the operating systems used, the application server and the web server must provide documentation and logging (logging) of information circulating in the System, protection of data from destruction in case of accidents and power failures of the System, control, storage, updating and recovery of data. The information content of the System (E-register data) is created during its operation, apart from a limited amount of initial data loaded during the preparation of the System for trial operation.

In the process of developing the system, it will be considered that all modules of the system must interact with each other.

Information in the system database should be saved in case of emergency situations.

Data backup should be carried out on a regular basis, in volumes sufficient to restore information in the data storage subsystem.

4.3.3. Linguistic requirements

When developing IS, high-level programming languages used for the development of information systems should be used.

The user interface should interact with the end user of the IS in three languages: Uzbek (Latin and Cyrillic), Russian and English.

When changing the language version of the IS, the user should remain on the original page, without automatically moving to the main page.

4.3.4. Software Requirements

Application software must meet the following requirements:

- high degree of readiness to solve the assigned tasks.
- compatibility of software products in terms of the used hardware, system software and system-wide infrastructure within the requirements for technical support, as well as their information compatibility within the requirements for information exchange.

The software must be developed taking into account the technology, ensure the implementation of all functions of the system and the solution of all tasks for each workstation.

The user interface "man-machine" for this IS should be carried out using the operator's workstation.

The operator's workstation should offer the operator a standard operating shell for the user. The operator must be provided with quick access to the necessary information. In the event of an error during data processing, the system must notify the operator immediately.

The software should be built in the form of software modules, unified for each workplace. At the same time, tasks that are not needed for this workstation should be inactive or added to the software shell. All modules must exchange information in full without damage to the entire system.

Access to information should be carried out in a timely manner, presented in the form of tables, reports, forms, corresponding main and context menus. Data must be transmitted over the network without affecting the functioning of the entire system. The system software should be able to create, maintain, use directories.

For the development of IS, the following list of technologies must be used:

• JAVASpring (to implement the IS backend);

• JAVAScript;

• Frameworks React.JS or Vue.JS (for the development of front-end IS);

• Development environment JDK, JRE J;

• JSON libraries;

• Springbot.

Server applications should be implemented using:

• Apachi;

• Xamp.

The functioning of the server side of the system must support OS Ubuntu, Sentos.

The database management system can be applied by agreement between the Customer and

the Contractor from the following options:

- PostgreSQL;
- Oracle.

The final list of technologies used is determined by agreement between the Customer and the Contractor at the stage of detailed design and based on the maximum efficiency of the work result.

4.3.5.Requirements for technical support

The composition of the equipment and the minimum requirements for the parameters of the equipment for the implementation of this project are provided below.

№ п/п	Required performance details	Required value
1	**2**	**3**
1.	Application server - 1 pc.	
1.1.	Rail kit for 19 "rack mounting	Required
1.2.	Number of supported processors, not less than	2
1.3.	Number of installed processors, not less than	2
1.4.	CPU clock speed, not less than	2.5 GHz
1.5.	Total volume L3 of processor memory, not less than	27,5 Mb
1.6.	The number of physical cores is not less than	20
1.7.	Number of logical cores: not less than	40
1.8.	Dynamic release of bad memory modules (ECC)	Required
1.9.	The number of DIMM slots is not less than	24
1.10.	RAM type	DDR4-2933
1.11.	RAM, not less than	512 GB
1.12.	Maximum amount of RAM expansion, not less than	6144 GB
1.13.	Using technology to correct errors	Required
1.14.	I / O bus type	PCIe
1.15.	Number of PCIe I / O slots, up to	6
1.16.	Network adapter 10 Gb / s 2-SFP + ports, not less than	1
1.17.	Network adapter 1 Gb / s, not less than	4
1.18.	Network adapter FC 16 Gb / s 2-ports, not less than	1
1.19.	Infiniband technology support	Required
1.20.	USB 3.0 at least	5
1.21.	Serial port at least	1
1.22.	Micro SD slot at least	1
1.23.	Internal HDD type	HDD SAS 10K 12Gbps 2.5in
1.24.	The number of internal HDD disks with a volume of at least	2

№ п/п	Required performance details	Required value
1	2	3
	1.2TB at least	
1.25.	Hot-Swappable Drives	Required
1.26.	RAID controller	PCI-E 3.0 Raid controller with 12 Gb / s SAS support per lane
1.27.	The RAID controller must support RAID	0, 1, 5, 6, 10, 50, 60
1.28.	The number of power supplies is not less than 500 W, not less than	2
1.29.	Power supply and fan redundancy	N + 1
1.30.	Hot-swap power supplies and fans	Required
2.	Database server - pcs.	
2.1.	Rail kit for 19 "rack mounting	Required
2.2.	Number of processors, not less than	2
2.3.	CPU clock frequency, not less than	3.6 GHz
2.4.	Total amount L3 of processor memory, not less than	24,75 Mb
2.5.	The number of physical cores is not less than	20
2.6.	Number of logical cores: not less than	40
2.7.	Dynamic release of bad memory modules (ECC)	Required
2.8.	The number of DIMM slots is not less than	24
2.9.	RAM type	DDR4-2933
2.10.	RAM, not less than	512 GB
2.11.	Maximum amount of RAM expansion, not less than	6144 GB
2.12.	Using technology to correct errors	Required
2.13.	I / O bus type	PCIe
2.14.	Number of PCIe I / O slots, up to	6
2.15.	Network adapter 10 Gb / s 2-ports SFP +, not less	1
2.16.	Network adapter 1 Gbps, not less than	4
2.17.	Network adapter FC 16 Gb / s 2-ports, not less	1
2.18.	Infiniband technology support	Required
2.19.	USB 3.0 at least	5
2.20.	Serial port at least	1
2.21.	Micro SD slot not less than	1
2.22.	Internal SSD drive type	SSD SAS Mixed Use 12Gbps 2.5in
2.23.	The number of internal SSD drives with a volume of at least 400 GB is at least	2
2.24.	RAID controller	PCI-E 3.0 Raid controller

№ п/п	Required performance details	Required value
1	2	3
		with 12 Gb / s SAS support per lane
2.25.	The RAID controller must support RAID	0, 1, 5, 6, 10, 50, 60
2.26.	Hot-Swappable Drives	Required
2.27.	The number of power supplies is not less than 800 W, not less	2
2.28.	Power supply and fan redundancy	N + 1
2.29.	Hot-swap power supplies and fans	Required

Data Storage requirements

The cache memory must be used to control information and store critical data.

The hardware platform must support 920/1920/3840/7680/15360 GB SSDs, 2/4/6/8 TB hard drives. The platform must support the replication functionality of the zero PRO embedded iSCSI / FCoE controller (SAS).

It is necessary to support SAN functionality, deduplication functionality, automatic SAN configuration functionality, SAN storage zoning functionality, data transfer functionality between multiple arrays, support for two types of SAS storage (SFF, LFF), data migration functionality.

There must be at least two controllers for increased reliability RAID 1, RAID5 and RAID6. Support for intelligent data placement by means of analysis of storage bottlenecks.

Hardware requirements:

№ п/п	Required performance details	Required value
1	2	3
1.	Data storage system - pcs.	
1.1.	Device type	Server cabinet mounted
1.2.	Unified storage	The proposed storage system should be a unified storage with one microcode / operating system;
1.3.	Supported operating systems	Storage must support the following operating systems: Windows Server 2016, Windows Server 2019, VMware, Solaris, HPE-UX, IBM-AIX, and Linux
1.4.	Disk space	The storage system must have a capacity of at least 288TB using disks no more than 8TB (at least 7.2 thousand rpm) and a capacity of at least 7.36TB SSD using disks no more than 920GB;
1.5.	Supported hard drives	The proposed storage system should support hot-pluggable 300/600/1200/1800 GB dual-port Enterprise SAS hard drives as

№ п/п	Required performance details	Required value
1	2	3
		well as 2TB / 4TB / 6TB / 8TB SATA hard drives; The proposed storage system must support SSDs with a capacity of more than 6 TB.
1.6.	Cache	The storage system must be provided with a minimum volume of 64 GB in one block; The cache should only be used for data and management. OS overhead does not have to run inside the cache; The proposed storage system should also be capable of additional Flash Cache support using SSD drives. Both file services as well as Block operations must be able to use flash cache. Recommended support for at least 800 GB of flash cache; If Flash is not supported internally by the storage, the vendor must ensure that the proposed storage can be scaled to a minimum of 128GB DRAM without replacing or upgrading controllers.
1.7.	Computing power	e proposed storage architecture should be based on a specially built ASIC engine, XOR, so that there is no load on the storage processor during Raid Parity calculations; In case the vendor does not have ASIC functionality, then an additional 16GB read / write cache must be provided for each control pair to balance performance.
1.8.	Architecture	Controllers must work in Active-Active mode so that one logical block can be distributed among all controllers in a symmetrical manner, with support for all basic functions such as Thin Provisioning, Data Tiering, etc.
1.9.	Points of failure	The proposed storage system must be configured in a No Single Point configuration, including controller board, cache, fans, power supply, etc.
1.10.	RAID support and virtualization	The proposed storage system must support RAID levels 1, 5, and 6; The proposed storage system should have built-in support for virtualization so that RAID 1, 5 and 6 can be stripped out of logical space, rather than having separate physical disks for each application; Each drive supplied must be able to participate in multiple and

№ п/п	Required performance details	Required value
1	2	3
		different RAIDs at the same time.
1.11.	Data protection	In the event of a power failure, the storage system must have a de-stage function to avoid data loss.
1.12.	Protocols	The proposed storage system must support all known protocols such as FC, ISCSI, FCOE, SMB 3.0, NFS V4, FTP / FTPS, etc.
1.13.	Host ports and Backend ports	The proposed storage system must have at least 12 host ports for connecting to servers at a speed of 16 Gbps; The proposed storage system must support additional IP ports of at least 4 10 Gbps ports or at least 8 x 1 Gbps for file services operations; The proposed storage system must have at least 2 additional IP ports for replication between storage systems. The proposed storage system must have at least 16 SAS Back-end lines operating at a speed of at least 12 Gbps per line.
1.14.	Performance and QoS (Quality of Service)	The proposed storage system should be able to group or RAID at least 30 hard drives for best performance. The proposed storage system must support QoS for mission-critical applications so that appropriate response times can be determined for application logical units in storage. It should be possible to define different service / response times for different logical units of the application. The QoS mechanism should be able to determine the minimum and maximum bandwidth for the required IOPS / bandwidth for the given logical units of the application running in the storage system. It should be possible to change the quality of service. Response time (in both milliseconds and submilliseconds), IOPS, real-time bandwidth specification.
1.15.	Provisioning and space allocation	The proposed storage system must support the modes of resource use "Thin Provisioning" and "Thin Reclamation" to keep the virtual disk "thin" for an extended period of time during operation. Thin Reclamation mode, the return of deleted (resettable, as is

№ п/п	Required performance details	Required value
1	2	3
		customary in the industry) blocks to the free space pool within the storage subsystem should be automated. Thin Reclamation operations should not cause a significant load on the central processing unit of the storage system and should ensure that blocks are returned to the free space pool even during peak loads on the array without significantly affecting its performance. For ease of management, Thin Provisioning functionality should be initially integrated into the array architecture, without the need to allocate separate pools of capacity for this functionality. The system must be capable of migrating from thick volumes from outside the array to thin volumes on the array. The system must support converting thick volumes to thin volumes and back on the array.
1.16.	Maintenance	The proposed storage system must support online (without interruption) firmware updates, both for the controller and for "hard" drives.
1.17.	Snapshot, copy, clone	The proposed storage system must have the functionality of "snapshots" (Snapshot) and also support the possibility of "full copies" (Clone);
1.18.	Control software	The proposed storage system should come with software for real-time monitoring of array performance through a graphical user interface.
1.19.	Storage Tiering	The proposed storage system must support background migration of a virtual volume from one type of RAID set to another type without interrupting the service of the application using the specified resource For efficient storage tiering, the storage system must support automatic policy-based data migration from one tier to another, including moving blocks of data by disk type (tier) within a single logical volume, between three tiers. As storage tiers, the customer should be able to use not only different types of media, but also the same type with different RAID levels and

№ п/п	Required performance details	Required value
1	2	3
		sizes.
1.20.	Remote replication	The data storage system must support the functionality of data replication at the controller level within the entire model range of the proposed array family The data storage system must be supported by a scheme of simultaneous synchronous and asynchronous replication, to support one reserve within the city (up to 10 km), and the second at a considerable distance (more than 100 km).

Purchase, delivery, adjustment of this equipment is not included in the present Terms of Reference and are provided by the Customer.

4.3.6.Requirements for metrological support

Requirements for metrological support will be determined depending on the equipment used and will apply to equipment and other technical means.

4.3.7.Requirements for organizational support

The organizational support of the IS should be sufficient for the personnel to effectively perform the duties assigned to them in the implementation of automated and related non-automated functions of the system.

Officials should be identified, which are responsible for:

- information processing
- administration
- ensuring the security of information
- management of the work of service personnel

Employees with personal computer skills, familiarized with operating rules, safety precautions and trained to work with an IS, should be allowed to work with this IS.

Mandatory instructions for users, including safety instructions, are required before starting work with the IS (and / or) subsystems.

4.3.8.Requirements for methodological support

The IS should be developed based on the current regulatory legal acts and organizational and administrative documents of the customer. Therefore, as part of the development of this IS, the

relevant administrative regulations of the customer must be considered, in which the processes of activity and functions of the departments, as well as employees of the customer's facilities, their rights, duties and responsibilities for using this system must be determined. Also, instructions on how users perform operations in working with the System must be approved in accordance with the established procedure. The composition of the methodological support will be specified in the process of software development and agreed with the Customer. Methodological support is provided at the request of the Developer and consists of:

- regulatory legal documents
- software user instructions
- job descriptions of personnel performing work using the System and its components.

5. The composition and content of work on the creation of the IS

The stages of creating an IS are presented in the Table below:

Stage No.	Name of works and their content	Execution Deadlines		Developer (organization, enterprise)	Stage completion result
		start	end		
1.	Development of Terms of Reference	March 2021	May 2021	UNDP	Terms of reference developed
2.	Passing the examination of the Terms of Reference at the State Unitary Enterprise "Center for Electronic Government Project Management" of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan	May 2021	May 2021	Customer, State Unitary Enterprise "Electronic Government Project Management Center" of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan	Expert opinions are received. TjR is approved
3.	Passing the	May 2021	May 2021	Customer, State	Expert

Stage No.	Name of works and their content	Execution Deadlines		Developer (organization, enterprise)	Stage completion result
		start	end		
	examination of the Terms of Reference at the State Unitary Enterprise "Cybersecurity Center" under the National Security Service of the Republic of Uzbekistan			Unitary Enterprise "Cybersecurity Center"	opinions are received. TjR is approved
4.	Conclusion of the Agreement	July 2021	July 2021	UNDP, Developer	A contract for the development of IS has been concluded
5.	Development	July 2021	September 2021	Developer	Demonstration of IS functionality in accordance with the Terms of Reference
6.	Testing	October 2021	October 2021	Customer, Developer	
7.	Drawing up operational documentation	October 2021	October 2021	Developer	Operational documentation prepared
8.	Examination of the software product for compliance with the Terms of Reference in the State Unitary Enterprise "Center for Management of Electronic Government Projects" of the Ministry of	October 2021	October 2021	Customer, State Unitary Enterprise "Electronic Government Project Management Center" of the Ministry of Information Technologies and	Expert opinions are received

Stage No.	Name of works and their content	Execution Deadlines		Developer (organization, enterprise)	Stage completion result
		start	end		
	Information Technologies and Communications of the Republic of Uzbekistan			Communications of the Republic of Uzbekistan	
9.	Examination of the software product for compliance with security requirements in the State Unitary Enterprise "Cybersecurity Center" under the State Security Service of the Republic of Uzbekistan	October 2021	October 2021	Customer, State Unitary Enterprise "Cybersecurity Center" under the State Security Service of the Republic of Uzbekistan	Expert opinions received
10.	Conducting trainings	October 2021	October 2021	Customer, Developer	Training provided
11.	Commissioning the software	Novermber 2021		Customer, Developer	Act of completed work, Act of putting the IS into operation

The customer must ensure the creation of conditions for the operation of the automation object, under which the compliance of the created IS with the requirements contained in the TK is guaranteed, namely:

- bringing the information entering the IS to a form suitable for processing using software and hardware (in accordance with the requirements for information and linguistic support)
- making the necessary changes in the automation object
- creation of conditions for the operation of the automation object, under which the

compliance of the created IS with the requirements contained in this Terms of Reference is guaranteed

- creation of subdivisions and services necessary for the functioning of the IS in the organizational structure of the Customer
- terms and procedure for staffing and staff training

When making changes to the IS, the following requirements must be met:

- all changes must be documented
- version compatibility must be maintained

6. Procedure for control and acceptance of the IS

During the delivery and acceptance of the project, the following types of work are carried out:

- Final tests of the IS
- elimination of defects
- IS acceptance tests

Verification and acceptance of the IS are carried out on the territory of the location of the objects of use of the product. The condition for the acceptance of the system - the IS must be prepared on a turnkey basis.

The IS tests are carried out in order to verify the compliance of the implementation of the TOR requirements, software operability, as well as to check the completeness of the software and documentation for hardware and software. The selection committee is formed from among the representatives of the organizations involved in the implementation of the project. The work on the implementation of the project is considered completed after the parties sign the acceptance certificate.

7. Requirements for the composition and content of work on the preparation of the IS for commissioning

7.1. Technical activities

In the process of creating an IS, it is necessary to perform the following set of activities to prepare systems for commissioning:

- to develop software necessary for launching the IS in trial operation, as well as operational documentation
- conduct training of personnel to work with IS

- to provide preparation of production areas for the placement of a complex of technical means
- to determine the persons responsible for the implementation of IS at the facilities
- to prepare the necessary organizational and administrative documents regulating the procedure for the work of personnel in the conditions of the functioning of the IS

The recruitment of the staff and departments necessary for the operation of the system, as well as the training of their employees, should be completed before the start of trial operation of the systems.

7.2. Bringing the information entering the IS to a form suitable for processing

Information is entered into the System by the user through filling in interactive web forms, each field of which is intended for entering data in a specific format, the correctness of filling in this case must be checked before saving the data in the IS.

7.3. Changes to be made in the automation object

As part of the implementation of the IS, the Customer needs the creation (or a corresponding change) of a specialized structural unit (department) of the automation object responsible for the administration and technical support. The composition of changes in the automation object should include:

- allocation and preparation of a special room for the placement of hardware components of the IS that meets the requirements given in this Terms of Reference
- installation and configuration of licensed software necessary for the functioning of the IS, in accordance with the software requirements given in this Terms of Reference
- installation and configuration of the developed IS components
- recruitment of personnel for the newly created subdivision of the automation object responsible for the administration and technical support of the IS
- training the users of the IS

7.4. Creation of conditions for the functioning of the automation object

It is necessary to ensure that the requirements for the operating conditions of the automation object and the characteristics of the environment specified in this subsection are met.

In addition, to ensure the compliance of the created IS with the requirements by the time of commissioning, the Customer must fulfill the requirements for the technical support of the IS, and

the users of the system must undergo training in working with it.

7.5. Creation of units and services necessary for the functioning of the IS

By the time the IS is transferred into operation, a system operation service must be created, which includes system Administrators and Information Administrators. Operations personnel must receive the required training.

7.6. Staff training

Before putting the software into operation, the Developer is obliged to prepare the User's Guide and the Administrator's Guide, as well as conduct training for the Customer's employees on working in the System and technical support based on this documentation.

7.7. Warranty service

The transfer of IS to warranty service occurs after the signing of the act of work performed under this Terms of Reference. Provides warranty service for IS for a period of 12 (twelve) months.

Warranty service includes:

- Correction of errors that occurred during the operation of the IS, within the framework of the developed functionality, approved by this Terms of Reference
- Consultations of the Customer's technical specialists on setting up the IS, on issues not covered in the technical documentation provided for the current project
- Consultations of operators on issues of work in IS, if the answers to these questions are absent in the developed and provided documentation on the current issue

Warranty service does not include:

- Implementation of work to improve the functionality of the IS not provided for by this Terms of Reference
- All additional requirements for functionality, database architecture, design, training for new users, and other issues not provided for by the current Terms of Reference are implemented under new Agreements.

To create the conditions for the functioning of the IS, under which the compliance of the created system with the requirements contained in this technical task is guaranteed, and the possibility of its effective use, a set of measures should be carried out in the organization of the Customer.

8. Documentation requirements

The composition of the technical documentation developed during the revision of the IS

components should include the following documents:

- Specification
- IS program code text (in electronic form)
- Installation instructions for the IS (as part of the IS Administrator's Guide)
- General description of the developed IS
- Program and methodology for testing the developed IS
- User's guide for the developed IS
- Administrator's Guide for the developed IS

The user manual should contain a description of the principles and functions of the IS, as well as methods of work at the operator's automated workstations.

The Administrator's Guide should include:

1. System deployment instructions
2. Description of the principles of the system organization (at the Administrator level)
3. Description of working methods
4. Description of methods for maintaining directories in the system database

By agreement of the parties and in connection with the training of the Customer's specialists by the Developer's specialists for the operation of the system in various modes of its operation, as well as in the case of concluding a contract for the maintenance of the system, the composition of the documentation may be limited by this Terms of Reference (determined by the Agreement on the creation of an IS)

All documentation should be provided to the Customer in 2 copies on paper and electronic (CD, flash) media. Electronic documents must be submitted in Microsoft Word 97-2016 format. The IS must be transferred to the Customer on electronic media (CD and flash) in two copies.

Documentation sets must be provided in Russian (English is allowed in those places where its presence is necessary).

9. Sources

1. O'zDSt 1985:2018 “Information Technology. Types, completeness and designation of documents when creating information systems”.

2. O'zDSt 1986: 2018 “Information technology. Information Systems. Stages of creation”.

3. O'zDSt 1987: 2018 “Information technology. Terms of Reference for the Creation of an Information System”.

Appendix A

The information system of electronic apostille and electronic register of certified documents “E-Apostille” and “E-Register”.

Name of the organization	Адрес
State Unitary Enterprise "Center for Management of Electronic Government Projects" of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan	Tashkent, st. Amir Temur shoh, 4 Phone: (+998 71) 238-41-07
State Unitary Enterprise "Cybersecurity Center"	Tashkent, st. Kirk-kiz, 10a Phone: (+998 71) 203-55-11