Extension of **"Automated Information System "FRONTIERA"**

Technical requirements for system extension and upgrade

Chisinau, 2021

Table of Contents

1 General information

1.1 Basic concepts and definitions

Automated information system "FRONTIERA" (hereinafter AIS "FRONTIERA") is an integrated automated information system of accounting and control of persons, vehicles, and goods (cargo) crossing the state and/or customs border of the Republic of Moldova. AIS "FRONTIERA" is an integral part of the National Information System of the Republic of Moldova located in the segment "Public Administration and Security" (fig. 1).

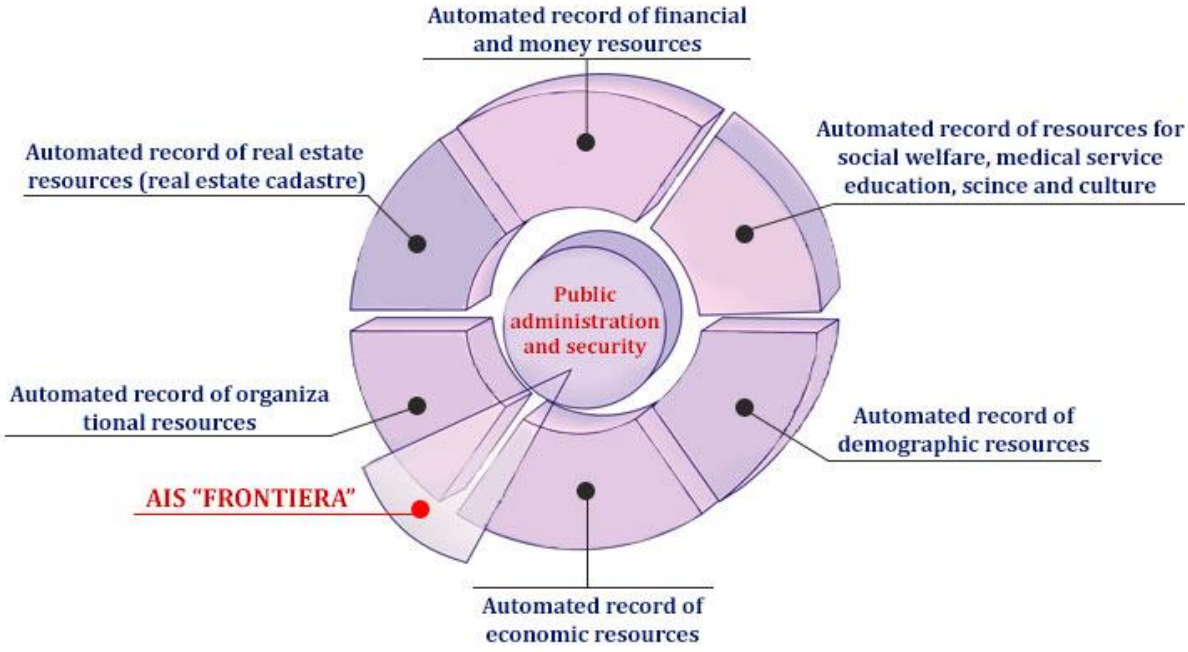


Fig. 1. The place of the AIS FRONTIERA» in the National Information System

State border is a line and a vertical plane going along the line determining the limits of the state territory (land, water, mineral) of the Republic of Moldova from the neighboring states.

Regime of the state border is a body of laws regulated by the law on the State Border of the Republic of Moldova and other regulations, contracts (agreements) concluded by the Republic of Moldova with neighboring states.

Border regime is a set of measures designed to create the necessary conditions for the protection of the State Border in the boundary strip, as well as in border waters and on the islands located on this territory in in accordance with the procedure established by the Government.

Border checkpoint is a place near railways, highway stations, river ports (quays), airports (aerodromes), open to international traffic, as well as other specially equipped places where

control is exercised, and the passage of persons, vehicles, goods (cargo) and other property across the state border is allowed.

Public authorities are created at **checkpoints** along the state border and contain boundary crossing points, customs, and other facilities that control the passage of persons, vehicles, goods (cargo), and other property crossing the state border.

There are three **types of checkpoints**:
- international (Chisinau Airport);
- interstate (Moldova–Romania);
- local (for residents of the border zone).

Customs border means the state border of the Republic of Moldova, perimeters of free zones, free customs warehouses.
The territory of the Republic of Moldova constitutes a single **customs territor**y, including land territory, internal waters, and the air space above them.

Customs regime is the legal framework that regulates the international traffic of the goods that are subject to the control of the customs.

Customs control is the process where customs inspects, verifies and examines inward and outward means of transport, goods, personal articles as well as mails and parcels according to the law to ensure the implementation of national laws and regulations concerning entry and exit of means of transport, goods, personal articles as well as mails and parcels through acceptance of declarations, document inspection, examination and release and other related management systems and procedures.

Customs declaration is an application of the established form in which the person specifies the customs procedure that must be applied to the goods and the information prescribed by the legislation about the goods, conditions and methods of their transportation.

Customs charges mean customs duties, taxes, duties and other mandatory charges levied by the customs bodies according to the law on the goods and means of transport carried across the customs border.

Single payment order is a consolidated document on the collection of cash payments accrued when crossing the state (customs) border by citizens and legal entities, regardless of their participation in foreign economic transactions.

Phytosanitary control is an inspection procedure applicable to plants and plant products when they are imported. The objective is to implement all measures for protection against the introduction of pests harmful to plants and plant products and against their spread.

Veterinary control is an inspection procedure applicable to animals and animal products when they are imported. The imported live animals and animal products present the highest level of risks as they can transmit serious human and animal diseases.

Sanitary and epidemiological control is a set of measures ensuring compliance with sanitary regulations, as well as compliance with mandatory requirements of state standards on safety for health and life of the population and the environment.

Environmental control is the state control for the toxicity and smokiness of exhaust gases of vehicles, regardless of their affiliation and forms of ownership in accordance with environmental legislation and current standards.

Vehicles include cars, buses, trucks (also with a trailer), motorcycles, mopeds, agricultural machinery, road construction equipment, railcars (passenger or freight), special-purpose cars, traction trains (electric locomotives, locomotives), boats.

Hereinafter, the word "**border**" means the state and/or customs border of the Republic of Moldova.

1.2 General provisions

The creation of the **Information System "Frontiera"** is based on Government Decree No. 1126 of August 28, 2002, On the approval of the Concept and Regulation on an automated information system to control persons, vehicles and goods (cargo) crossing the state and/or customs border.

According to the Concept, the following services were located in the control zone to carry out calculations of border payments and taxes:

Frontier Service was responsible for the route opening by entering data on the vehicle and its driver, document control, then based on the confirmation of all services located in the control zone, and it also issued an exit permit;

National Agency for Road Transport (ANTA) was responsible for entering information about the calculated amounts of taxes, roads into the information system;

Sanitary and Veterinary Agency is responsible for entering data on issued documents, results of inspections, and calculated amounts into the system;

Phytosanitary Inspection was responsible for entering data on issued documents, results of inspections, and calculated amounts into the system;

Customs Service is responsible for entering vehicle data, information about the goods transported into the information system, forming a single payment voucher and its transferring to the M-Pay payment system API;

Bank is responsible for confirming the receipt of payment and returning payment confirmation to the information system through the API.

Ministry of Agriculture and Food Industry, Main State Inspectorate on Phytosanitary Quarantine, National Agency for Road Transport and Customs Service of the Republic of Moldova regulated the procedures for optimizing the passage of the state border by road

transport with goods, which are subject to sanitary control - veterinary and phytosanitary, environmental payments, ANTA transport documents verification - on the principle of a **single window**, defined in Government Decree No. 1073, dated 19 Sept. 2008 "On the Way to Optimize the State Border Crossing by Road Transport with Cargo and Passengers" and Joint Decree No. 202/68/372, dated 17 Oct. 2008.

Thus, the Customs Service instructed the State Enterprise "Vamtehinform" as soon as possible to develop a tool for the automatic calculation of environmental fees and road charges, that would subsequently be available to customs inspectors at border posts. Based on clearly defined requirements for the functionality of the new system, the absence of any forward-looking requirements when developing the system, led to the creation of a system based on structured programming using the Java programming language and WEB technologies.

Over time, the IS "Frontiera" has undergone a large number of enhancements to the functionality of the system. IS "Frontiera" was not designed as a modular system and, as a result, any functional addition requires more human resources and time. At the same time, new functionalities operate along the same one-step principle.

The principles, implemented in the IS "Frontiera", did not offer management, configuration, security, administration, system audit, it did not provide for the extension of the system by new modules.

As a result, we are forced to state that the new requirements for the existing IS Frontiera cannot be met without revising the technology and principles on which it was created. The structure of the current state of the IS "Frontiera" is presented below.

This document contains the technical and quality characteristics of the system, the list and reporting terms of services for the development and implementation of a management system of vehicle checkpoints. The requirements specified in this document are not exhaustive and may be clarified or not significantly changed during the product development process.

The implemented system should conform to the following basic requirements:
- web-oriented;
- universal;
- functionally complete;
- reliable (autosave without data loss);
- scalable and upgradable;
- modular;
- intuitive user interface;
- protected from external influences;
- to log all users' actions.

1.3 Regulatory documents used to create the system

The purpose of the formation of the regulatory and legal framework of the AIS "FRONTIERA" is to create the necessary organizational and legal conditions that ensure the development

and use of a comprehensive integrated automated information system for accounting and control of persons, vehicles and goods (cargo) crossing the border of the Republic of Moldova. Legal support of the AIS "FRONTIERA" is based on normative legal acts regulating the existing system of accounting and control of objects to be registered, as well as processes of informatization and formation of a single information space of the Republic of Moldova.

The main normative legal acts regulating the creation and operation of the AIS "FRONTIERA" are:

- The Constitution of the Republic of Moldova;
- Law No. 1513-XII of June 16, 1993, On Sanitary and Epidemiological Provision of the Population;
- Law No. 108-XIII of May 17, 1994, On the State Border of the Republic of Moldova;
- Budget Law (adopted annually);
- Law No. 273-XIII of November 9, 1994, On Identity Documents of the National Passport System;
- Law No. 275-XIII of November 10, 1994, On the legal status of foreign citizens and stateless persons in the Republic of Moldova;
- Law No. 506-XIII of June 22, 1995, On Phytosanitary Quarantine;
- Law No. 618-XIII of October 31, 1995, On State Security;
- Law No. 269-XIII of November 9, 1995, On Exit from the Republic of Moldova and Entry to the Republic of Moldova;
- Customs Code adopted by Law No. 1149-XIV of 20 July 2000;
- Law of the Republic of Moldova No. 440-XV of July 27, 2001, On Free Enterprise Zones;

Decisions of the Government of the Republic of Moldova:

- No. 496 of September 6, 1991, On the establishment of checkpoints and customs points;
- No. 1052 of November 8, 1999, On the regulation of services activities at border checkpoints;
- No. 808 of August 9, 2000, On the interaction of services, streamlining the collection of payments and automation of the accounting system at checkpoints on the state border of the Republic of Moldova;
- No. 903 of August 30, 2001, On the development and implementation of an information system for accounting and control of transit traffic;
- No. 1009 of September 27, 2001, On the pre-shipment inspection of imported goods;
- Regulations of July 18, 1996 (Ministry of Transport and Communications), On posts of environmental control and diagnostics of vehicles in the territory of the Republic of Moldova;
- Other departmental regulations.

At the same time, the creation and effective functioning of the AIS "FRONTIERA" require the adoption of new laws and improvement of the current legislation that would regulate relations arising from the collection, processing, storage, sharing and protection of data, as well as establish the legal regime for the operation of the AIS "FRONTIERA".

2 Purpose and objectives of the system

The AIS "FRONTIERA" was created primarily to ensure the security of the Republic of Moldova, in particular by preventing illegal import and export of goods, falsification of goods and

forgery of documents, monitoring illegal migration, identifying persons and vehicles prohibited from entering and leaving the country.

The main objectives of creating the AIS "FRONTIERA" are:

- ensure the economic sovereignty of the Republic of Moldova by establishing a transparent land border;
- increase revenues to the national budget via control over the import-export and transit of goods;
- improve the stability of the state by registering and checking individuals crossing the border, and controlling the influx of foreign citizens and stateless persons;
- strengthen the fight against crime by effective counteracting organized crime, illegal migration, drug trafficking, illegal transportation of weapons and other illegal acts at the border crossing points;
- increase the throughput of checkpoints;
- ensure effective cooperation and interaction between interested ministries and departments on registration and control.

2.1 The purpose of the system

The AIS "FRONTIERA" was created on the following basic principles:

- the principle of the **system legitimacy**, which implies the creation and use of the AIS "FRONTIERA" in accordance with the provisions of the national legislation in force;
- the principle of **observance of human rights**, which provides for the operation of the system in strict accordance with national normative documents, including human rights treaties and agreements to which the Republic of Moldova is a party;
- the **person-centered** principle requires a high-ranking manager with sufficient authority to make decisions and coordinate work on the creation and operation of the system;
- the principle of the **validity of system data** requires the entry of data into the system only on the basis of records in documents accepted as a source of information;
- the principle of **data integrity, completeness, and reliability** where:
- the **data integrity** is understood as the state when data keep the content and unambiguous interpretation under the influence of random factors. The data integrity is considered to be preserved if it is not corrupted or destroyed (not erased);
- the **completeness of data** means the amount of information collected about the objects of accounting and control of the system in accordance with regulations;
- the **data reliability** is understood as the degree of compliance of the information, stored in the computer memory or in documents, to the real state of the objects displayed in the system;
- the principle of **state identification of registration object**s, according to which the objects of identification are individuals, vehicles crossing the border, each of which is checked for the state identification number (for example, for natural persons - the state identification number of the natural person, and for legal entities - state identification number of the legal unit);
- the principle of **control over formation and use of the system**, implemented through a number of technical and organizational measures and application programs, designed to ensure the high quality of state information resources, high reliability of

their storage and management, including the correct use in accordance with the standards provided within the current legislation.

2.2 System outcomes

System allows:

- to significantly speed up the process of crossing checkpoints by vehicles.
- to improve security by preventing vehicles and persons with law enforcement concerns from entering or leaving;
- to have a tool to control the location of a vehicle at checkpoints;
- to have a tool for online monitoring and work with archives at checkpoints;
- to minimize the human factor impact;
- to ensure the transparency of the activities of customs authorities at checkpoints;
- to ensure the transparency of the activities of customs authorities at checkpoints;
- to unify the data that should be recorded by system users for each vehicle crossing the border.

2.3 Tasks of the AIS "FRONTIERA"

The AIS "FRONTIERA" is assigned the following tasks:

- to provide the leadership of the republic with accurate and timely information on the entry/exit of persons and vehicles and the import/export of goods, necessary in order to take the necessary well-thought-out decisions at the state level;
- to provide automated record and control of persons, vehicles and goods crossing the border;
- to provide automated record and control of submitted documents;
- to identify persons who do not have the right to enter and leave the Republic of Moldova, as well as vehicles and goods that are prohibited from entering or leaving the country;
- to increase the throughput of checkpoints using machine-readable documents and computer guides;
- improve the service level by speeding up the registration process control and collection of customs duties and taxes;
- to create a single integrated data on border crossing by persons, vehicles and goods;
- to support departmental information systems with accurate and timely information on border crossing by persons, vehicles and goods;
- to ensure the operation of the system on a full-time basis.

2.4 System Development Procedure

2.4.1 Components of core software upgrade / Frontiera

The main purpose of the AIS upgrade is to implement a microservice architecture instead of a monolithic one and replace the application server in order to provide scalability and increased security. Scalability is achieved by implementing a microservice model. In practice, there will be no need to rebuild the core of the system every time in order to add or change

the functionality of any of the modules. This, in turn, will reduce the costs of developing and maintaining the system, it will also be possible to involve different development teams for small tasks. The existing solution, JBOSS, is already out of vendor support, it means that vulnerabilities are NOT monitored or patched. In practice, it increases the software vulnerability, which has to be compensated for additional costs (i. e. to buy more expensive network hardware and software to protect against threats in proportion to the core system vulnerability).

Stages of development
Upgrade of the application architecture and the replacement of the application server
Upgrade of the report designer
Upgrade of automated information exchange module
Migration of the module for exchanging information with other participants of MConnect (ministries, authorities)
Module "Auto" will take data from Frontier Police or manual registration, or from other external systems (registration plate readers, electronic ticket systems, etc.), and add data for further processing
Module "ANTA" provides for checking documents, issued by "AHTA" for international transportation, and calculation of road taxes in accordance with the current legislation
Module "Bank" is accounting of taxes and customs payments, exchange of information with Web Service "Single window of customs service for payment"
Module ANSA (National Food Safety Agency)
Module Veterinary service

There have been changes in the legislation of the Republic of Moldova regarding the rules of interaction between state information systems as of 2021. The system MConnect was implemented (https://www.egov.md/ru/projects/mconnect).

The Interoperability Governmental Platform MConnect facilitates the exchange of data between the authorities to increase the efficiency and quality of delivery of public services. Through the interoperability platform, the public authorities exchange data in real time that reduces the number of requested documents from individuals and legal entities (certificates, reports, etc.).

Advantages:
- increase the efficiency and effectiveness of information systems through which electronic public services are delivered;
- increase the efficiency of the use of public funds;
- increase citizens' comfort;
- increase the security of information systems of the local and central public administration;
- reuse the resources involved in the information systems;
- improve the collaboration between the institutions of public administration;
- promote the web accessibility.

In connection with this legislative initiative, the exchange with external systems cannot be carried out in the existing system considering that the existing platform did not exist initially.

Currently, **the exchange shall be performed through the MConnect** platform. It requires upgrading the system, namely modules for exchanging information between participants within the country and with external partners.

2.5 Services order of execution

In addition to the comprehensive modernization of the system core, the scenario includes updating of key modules required for the customs service of the Republic of Moldova.

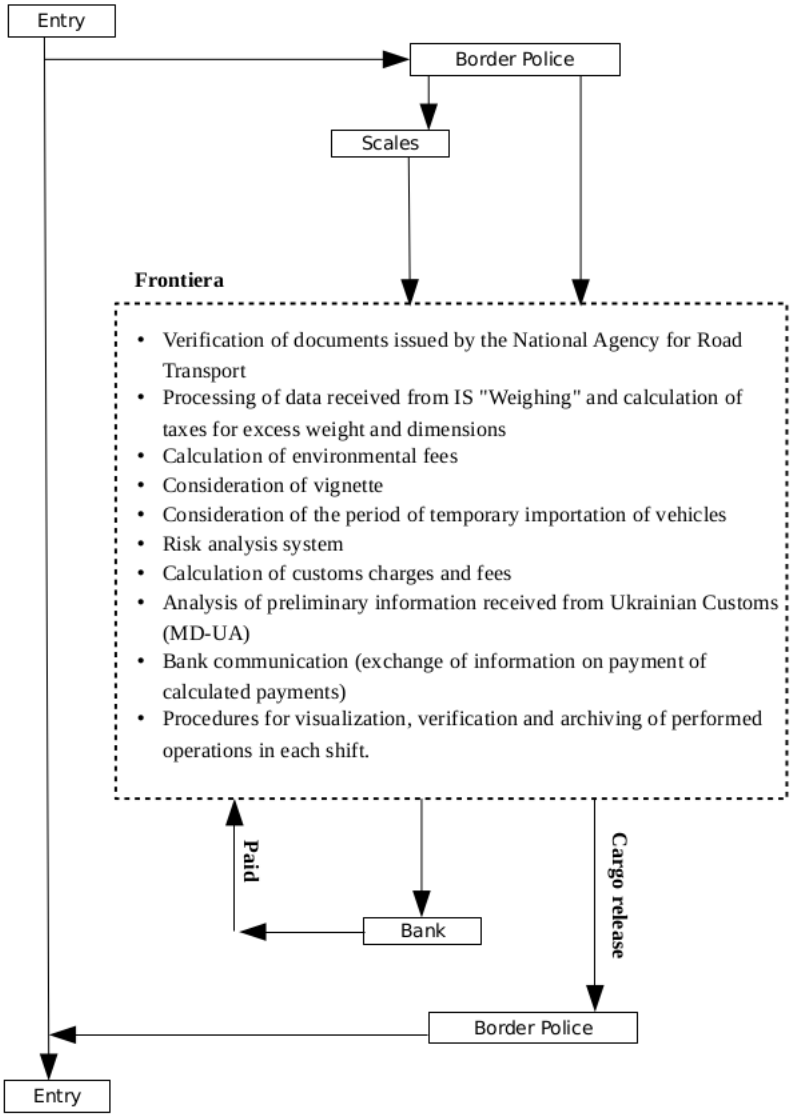
Expected result:
- a comprehensive upgraded core system will be designed to achieve exceptional flexibility, ease of management, reliability and security;
- algorithm and control mechanism of the integrated video surveillance system, including ANPR and video surveillance;
- compliance of AIS with modern safety requirements Top 10 OWASP;
- a new module created in accordance with the requirements of the legislation; mechanism of electronic interaction between other government agencies, including the implementation of MConnect;
- modernized module of information exchange with Ukraine.

3 General requirements of the system

3.1 System functionality description

The system should ensure the creation, updating, filling of records on the movement of vehicles at the checkpoint and the implementation of the related functionality.

3.2 Structure and function scheme



3.3 Description of system user roles and access

The user role model should be constructed within the system with the ability to differentiate access rights and the ability to create an unlimited number of users for each role.

3.4 Technological stack

To achieve exceptional flexibility, ease of management, reliability and safety, the most proven, modern and affordable technologies were selected from existing technologies. It should also be noted that the implementation of new components into the integrated information system of the Customs Service of Moldova can replace some of the existing ones, but on the condition the functionality is saved and there is no drop in productivity. So, a virtualization technology based on Docker + Kubernetes was chosen. It is also proposed to replace the monolithic JBOSS architecture with a service architecture and develop a user interface with the modern solutions, for example, replacing JSP with React. All these measures should lead to the creation of a so-called future proof system that will be used for

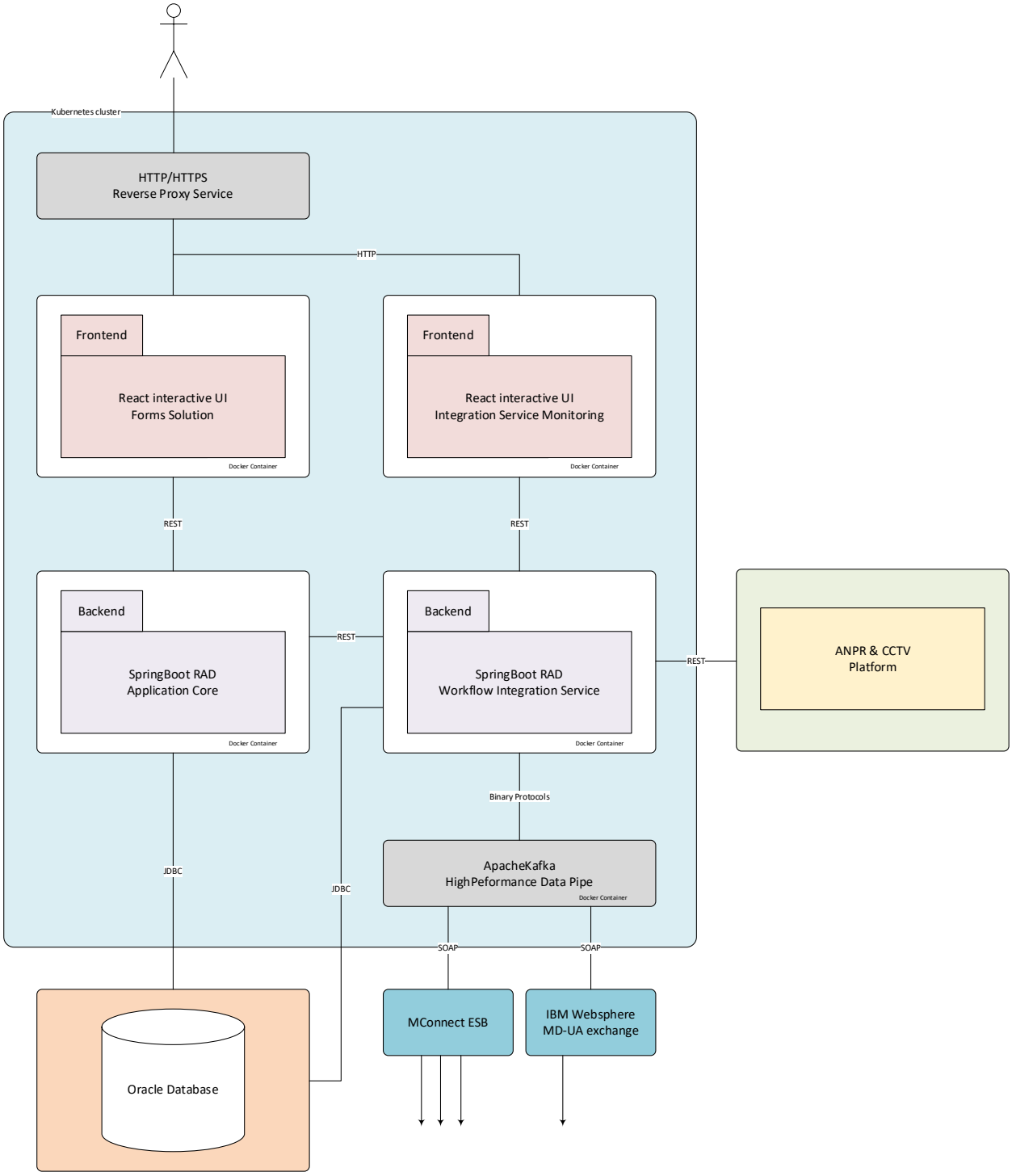
a long time, provide reusable components and improve the overall quality of the information system of the Customs Service of the Republic of Moldova.

Technologies:

- **Proxy Server** – a reverse proxy server is required to connect users from the external network securely and resilient.
- **Kubernetes cluster** is required for automating deployment, scaling of Docker containers.
- **Docker container** is an application with all its environment and dependencies, which can be easily managed: transfer to another sever, scale, update.
- **Frontend/Backend** is a modular approach based on the use of distributed, loosely linked components, equipped with standardized interfaces for interaction on standardized protocols.
- **Apache Kafka** is a distributed, horizontally-scalable system that provides throughput with even increasing load. It also supports the ability to store data for subsequent batch processing. One of the features is the use of a technique similar to transaction logs used in database management systems, allowing to protect and guarantee data delivery.
- **React** is an open-source library for building user interfaces. Its goal is to provide high speed, simplicity, and scalability.
- **Spring Boot** is a set of tools for creating stand-alone, production-grade Spring-based Applications that you can "just run".

Functional components:

- **Forms Solution** is a modern web-application that includes custom ANPR & CCTV access capabilities, etc.
- **Integration Service Monitoring** is an application for monitoring data exchange processes and general system parameters.
- **Application Core** is an application that provides an abstraction of business logic, provides interfaces for custom applications.
- **Workflow Integration Service** is an application that provides data aggregation and processing for communication with external systems, including ANPR & CCTV.
- **ANPR & CCTV** is an external system that integrates standard interfaces. Accessibility for this integration is provided through the Workflow Integration Service.


Kubernetes cluster
HTTP/HTTPS
Reverse Proxy Service
HTTP
Frontend
React interactive UI
Forms Solution
Docker Container
Frontend
React interactive UI
Integration Service Monitoring
Docker Container
REST
REST
Backend
SpringBoot RAD
Application Core
Docker Container
REST
Backend
SpringBoot RAD
Workflow Integration Service
Docker Container
REST
ANPR & CCTV
Platform
Binary Protocols
JDBC
JDBC
ApacheKafka
HighPeformance Data Pipe
Docker Container
SOAP
SOAP
Oracle Database
MConnect ESB
IBM Websphere
MD-UA exchange

4 Functional requirements

4.1 Basic functions

The basic functions of the AIS "FRONTIERA" are:
a) the formation of a database, including the functions of the initial registration of an object, data updating and de-registration. These functions are carried out during the collection of data on accounting objects, issuance of customs documents during registration, as well as during information exchange with the state authorities and local public administration authorities.

Information is entered into the data bank of the AIS "FRONTIERA" only on the basis of documents confirming the accuracy of information on the accounting object, with a clear reference to the document based on which the data was updated.
b) organization of information exchange from the database;
c) ensuring the quality of information by establishing and maintaining quality system components;
d) comprehensive support of the AIS "FRONTIERA"

Specific Functional Requirements for the extension and upgrade of the AIS “Frontiera” are included in Annex A: Functional Requirements

4.2 Documents of AIS "FRONTIERA"

Documents recorded in the AIS "FRONTIERA" are divided into the following categories:

- identity documents;
- legal entity document;
- driver's documents;
- vehicle documents;
- accompanying documents for goods (cargo);
- single payment order;
- documents of the State Sanitary and Epidemiological Service;
- documents of the State Veterinary Service;
- documents of the State Phytosanitary Quarantine Service;
- documents of the State Environmental Inspection;
- technological documents.

4.2.1 Identity documents

Identity documents include:

- identification documents of national passport system of the Republic of Moldova:
    - passport of the citizen of the Republic of Moldova;
    - diplomatic passport;
    - service passport;
    - passport of a stateless person;
    - identity card of a citizen of the Republic of Moldova;

- identity card of a stateless person;
- permanent residence permit of a foreign citizen permanently residing in the Republic of Moldova;
- temporary residence permit of a stateless person;
- temporary residence permit for a foreign citizen;
- seaman's passport;

- national passports of foreign citizens;
- certificate of the embassy of a foreign state in Moldova, issued instead of the lost document;
- Certificate for return to the Republic of Moldova.

4.2.2 Legal entity document

When crossing the border, the representative of the legal entity submits the following documents:
- machine-readable registration card of the legal entity;
- contract or a copy of the contract;
- registration documents of a foreign legal entity.

4.2.3 Driver's documents

When crossing the border, the driver of a vehicle is obliged to submit a driver's license.

When performing international road transport operations, including transit, the driver should additionally submit the following documents:
- certificate of registration of carrying foreign currencies by employees or foreign currency import certificate;
- medical certificate of driver's health;
- individual control book (in the absence or malfunction of tachograph);
- certificate of an international driver (CIPTI center);
- driver certificate of professional competence (for the transport of dangerous goods only).

4.2.4 Vehicle documents

When crossing the border in a vehicle, the following documents are required:
- vehicle registration certificate;
- inspection ticker;
- certificate of civil liability insurance;
- a customs certificate (issued for the initial import of a vehicle into the Republic of Moldova).

When performing international road transport operations, including transit, the driver should additionally submit the following documents:
- certificate of suitability of the vehicle for the international carriage of goods (cargo), under the terms of the TIR convention (with photos);
- permit for transportation through foreign territory;
- certificate of admission of a vehicle to the carriage of dangerous goods (for the transport of dangerous goods only);
- licensed machine-readable card;
- waybill (a copy of the contract for carriage or a revenue account book);
- carnet de passages (for states where it is required).

When crossing the border by rail, a transfer sheet is submitted (for each train).

4.2.5 Accompanying documents for goods (cargo)

When carrying out transportation (including in transit), the following accompanying documents for the cargo are additionally submitted:

- application for pre-shipment inspection of imported products;
- report on positive results of inspection or discrepancy report (used by the customs authorities of the Republic of Moldova to simplify the processing of customs documents when importing material assets), a security label (for payment);
- customs declaration for a legal entity;
- customs declaration for an individual;
- certificate of origin, quality and conformity of goods;
- invoice in which the quantity and value of goods are indicated;
- consignment note for goods, transport is indicated (road, air, rail, etc.);
- authorization for a person who is engaged in the import/export of goods;
- CMR waybills with specifications and other necessary accompanying documents;
- TIR Carnet;
- carrier's liability insurance (copy of the insurance policy);
- certificate of the Chamber of Commerce and Industry.

4.2.6 Documents of the State Sanitary and Epidemiological Service

- various certificates.

4.2.7 Documents of the State Veterinary Service

- veterinary certificate;
- sanitary permit.

4.2.8 Documents of the State Phytosanitary Quarantine Service

- phytosanitary pass;
- sanitary permit.

4.2.9 Documents of the State Environmental Inspection

- environmental certificate.

4.2.10 Technological documents

- various certificates;
- various analytical and statistical reports;
- certificate of accompanying.

4.3 Information space of the AIS "FRONTIERA"

Like any other information system, the AIS "FRONTIERA" is designed as an indivisible core, which includes the data of all accounting and control objects and the scenarios by which they interact (fig. 4). Data field is generated by activating the attributes of these objects as a result of their interaction according to standard cyclical scenarios.

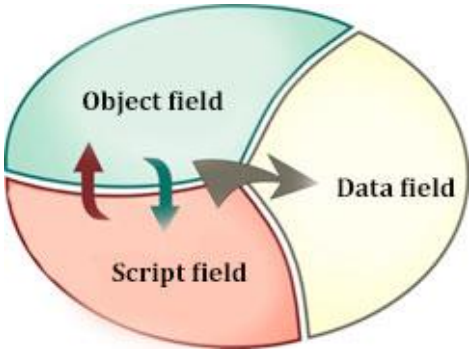


Fig. 4. The information core structure of the AIS "FRONTIERA"

4.3.1 The objects of accounting and control of AIS "FRONTIERA" are:

1) trip is a concept that combines:

- fact of crossing the border;
- vehicle crossing the border;
- an individual driving the vehicle;
- individuals – passengers of the vehicle;
- goods (cargo) transported by the vehicle;
- legal unit responsible for the relevant goods (goods) (shipper/recipient, owner of the goods).
    - Crossing the border on foot or by bike is also considered a separate trip;

2) Individuals of the following categories:

- foreign citizens and stateless persons permanently residing on the territory of the Republic of Moldova;
- citizens of the Republic of Moldova permanently residing abroad;
- citizens of the Republic of Moldova entering or leaving the Republic of Moldova;
- foreign citizens and stateless persons temporarily staying in the Republic of Moldova;

3) Legal units of the following categories:

- public authorities;
- enterprises;
- public associations;
- parties and political and social organization;
- trade unions;
- cooperatives (associations of cooperatives);
- parts of religious cults;
- associations of co-owners in the condominium;

4) vehicles:

- cars (including with a trailer);
- buses
- trucks (including with a trailer);
- motorcycles;
- agricultural machinery, road construction equipment;
- railcars (passenger or freight);
- special-purpose cars;

- traction trains (electric locomotives, locomotives) crossing the border on its own or by towing;

5) goods (cargo).

6) documents:
- identity documents;
- visa regime documents;
- legal entity documents;
- driver's documents;
- vehicle documents;
- documents for goods (cargo);
- single payment order;
- documents of the State Sanitary and Epidemiological Service, the State Veterinary Service, the State Phytosanitary Quarantine Service and the State Environmental Inspection.

7) forms of strict reporting documents.

4.3.2 Objects identification of the AIS "Frontiera"

The main identification features of each object of accounting and control of the AIS "Frontiera" are the trip identification, the state identification number of the natural person (IDNP), the state identification number of organization (IDNO), vehicle identification number (VIN), product code by product nomenclature.

Trip identification

The trip identifier is a strictly defined sequence of 13 digits (fig. 5):

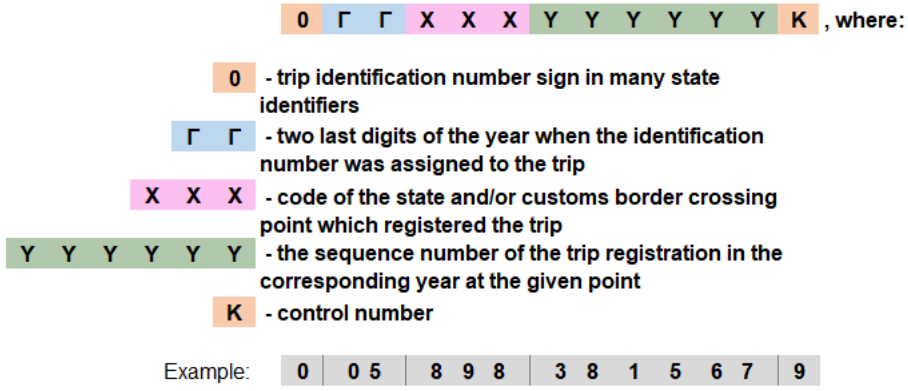


Fig.5. Trip ID character content

Individual identification

The state identification number of the natural person is the basic identification of an individual, and a strictly defined sequence of 13 alphanumeric characters (fig. 6).

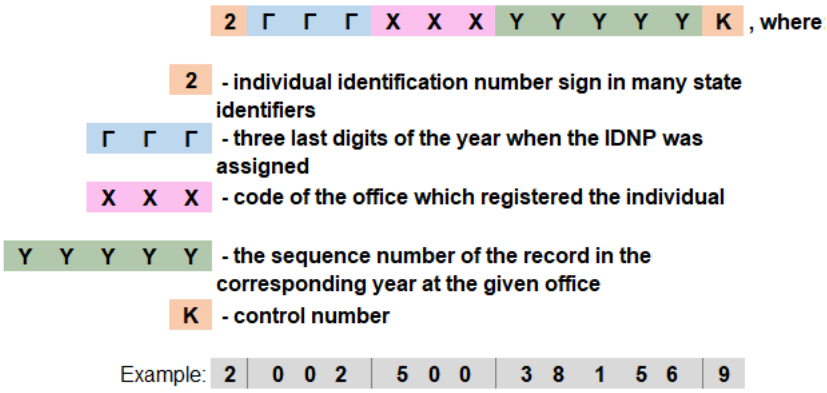


Fig.6. Content of characters of the State identification number of the natural person
Identification of a legal entity

Identification of legal unit

The main identifying feature of a legal unit is the state identification number of organization (IDNO), which is a strictly defined sequence of 13 alphanumeric characters (fig. 7).

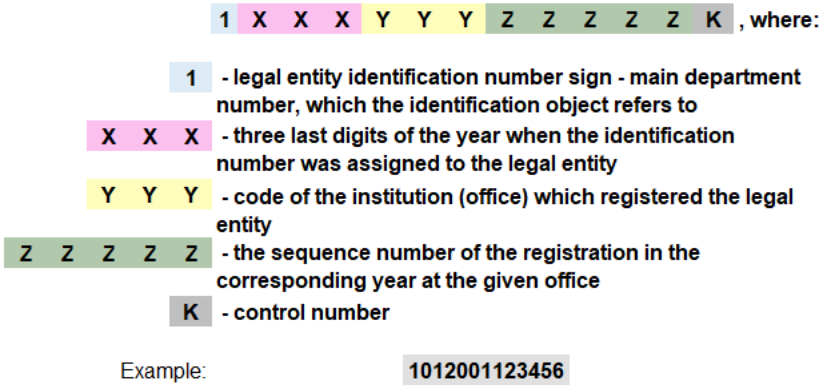


Fig. 7. Content of characters of the State identification number of organizations

Vehicle identification

The main identification feature of a vehicle is the vehicle identification number (VIN), which is a unique vehicle number applied by the manufacturer, according to ISO 3779-76 “Cars. International identification number "and ISO 3780-76" Cars. International identification code of manufacturers" (fig. 8).

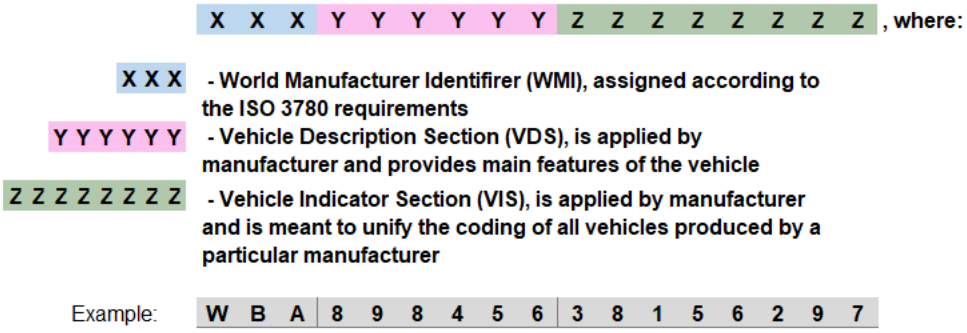


Fig. 8. VIN character content

If the VIN is not affixed by the vehicle manufacturer, falsified or destroyed, it is assigned and applied when issuing a permit for operation.
Numbered units are identified as follows:
type + number

Identification of goods (cargo)
The identification of goods is carried out by coding, according to the national nomenclature of goods. The code is a strict sequence of 9 digits (fig. 9):

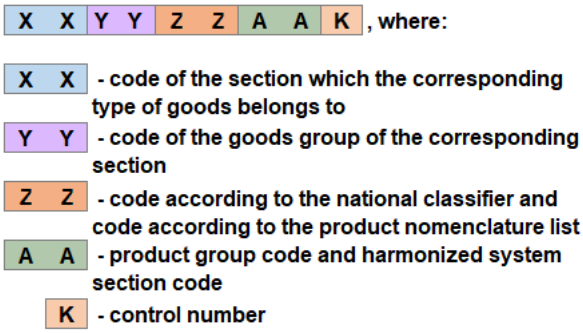


Fig.9. Contents of the product code of goods (cargo)

The method of identifying a unit of goods will be determined after the development of the automated information system "Turnover".

Identification of documents and forms of strict reporting

Identification of documents and forms of strict reporting is carried out by a combined key, which includes the following elements:
document code + series + number

4.3.3 Basic scenarios

The implementation of the functions of the AIS "FRONTIERA" in the course of accounting and control of objects when crossing the border is carried out according to the following basic scenarios:

1) trip:
- identification (assignment of an identification number);
- trip identification;
- implementation of scenarios for trip participants;
- making all payments under a single payment order;
- making decisions on a trip based on decisions taken by its participants;
- entering information into the database;

2) individual:
- identification (if it does not appear in the State Register of Population, registration with the assignment of IDNP);
- registration of a visa (if necessary, in the absence);
- determination of the status of a person on the trip;
- determination of the motive for crossing the border;
- control of submitted documents;
- documents check by filter arrays;
- check if filling out a customs declaration for an individual (if necessary);

- making a decision on an individual;
- entering information into the database;

3) legal unit:

- identification (if there are no legal units in the State Register, registration with the assignment of IDNO);
- determination of the role of the legal unit in the trip and its powers;
- control of submitted documents;
- documents check by filter arrays;
- making a decision on a legal unit;
- entering information into the database;

4) vehicle:

- identification (if it is not in the State Register of Transport, registration in this register);
- determination of the motive for crossing the border;
- control of submitted documents;
- documents check by filter arrays;
- implementation of various types of control and processing of relevant documents;
- calculation of due ANTA payments;
- making a decision on a vehicle;
- entering information into the database;

5) goods (cargo):

- identification (identification code of goods);
- determination of grounds for crossing the border;
- control of submitted documents;
- check if filling out a customs declaration for a legal unit;
- implementation of various types of control and processing of relevant documents;
- sealing (at the entrance to the checkpoint) and security seal control (when leaving);
- calculation of other customs payments (payment for seals);
- making a decision on the product;
- entering information into the database;

6) documents:

- identification;
- control;
- seizure if necessary;
- invalid marks;
- entering information into the database.

The implementation of scenarios is carried out by employees of the relevant services, according to the current law and departmental orders and instructions

4.3.4 The AIS "FRONTIERA" contains the following data

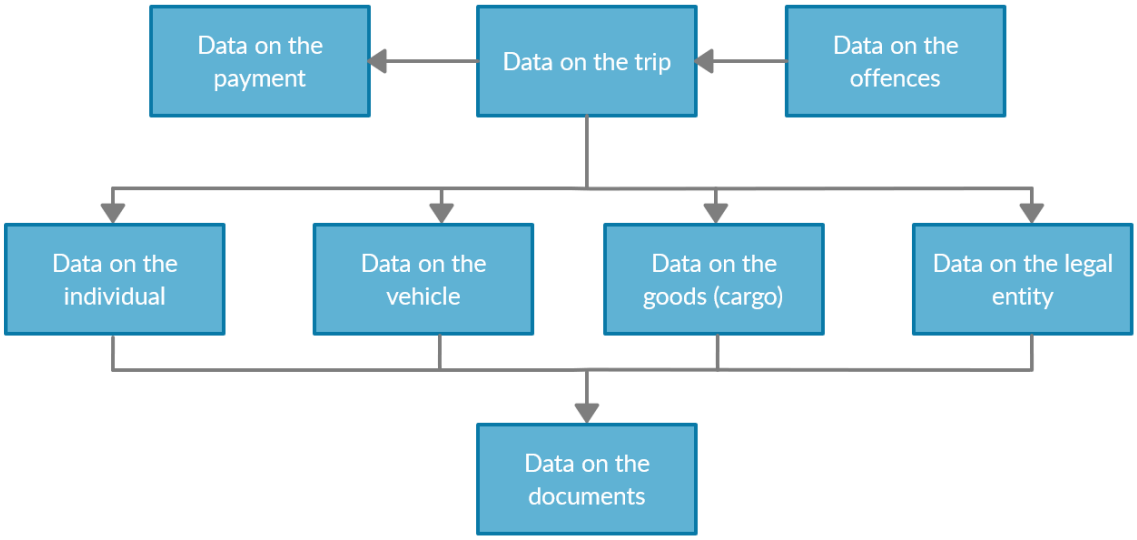


Fig. 10. The data contained in the AIS "FRONTIERA

(1) trip data:
- trip identifier;
- date and time of border crossing;
- checkpoint;
- entering and leaving the country;

(2) information about an individual:
- the state identification number of the natural person (IDNP);
- personal identification data:
- last name;
- name;
- father's name (patronymic);
- sex;
- date of birth;
- place of birth;
- citizenship data;
- motive of border crossing;
- reference to an individual with whom a citizen who does not have his own document crossed the border;
- category of person (driver, passenger accompanying another person, accompanying the cargo);
- country of consignment/destination;

(3) data on the legal unit:
- the state identification number of organization (IDNO);
- identification data:
- name of the legal unit;
- legal category;
- organizational and legal data:
- type of property;
- organizational and legal form;

- acts as a legal unit when carrying out operations with goods (cargo);

(4) vehicle data:

- VIN;
- vehicle type;
- vehicle make-model;
- body number;
- chassis number;
- engine number;
- registration plate;
- type of registration plate;
- specifications;
- country of registration of the vehicle;
- motive of border crossing;
- owner details:
    - individual;
    - legal unit;

(5) goods (cargo) data:

- product identification code;
- product name;
- quantity of goods;
- cost of goods:
- unit:
    - basic;
    - additional;
- internal customs code;

(6) payment details:

- payment type;
- amount;
- payer;
- terms of payment;

(7) document details:

- type of document;
- series;
- number;
- data of issue;
- issuing authority;
- validity;

(8) data on offences:

- type;
- date of commission;
- enforcement action;

(9) digital map layer:

- state border line;
- customs border line;
- border checkpoint;
- internal customs;
- customs warehouses;
- free enterprise zones.

4.3.5 Classifiers

In order to ensure the reliability of information and reduce the amount of data stored in the AIS "FRONTIERA", a system of classifiers is used, which can be divided into three categories:

- international classifiers;
- national classifiers;
- internal classifiers.

Within the AIS "FRONTIERA", internal system classifiers are developed and used only in the absence of approved international and national classifiers.

4.4 Information platform of the AIS "FRONTIERA"

The AIS "FRONTIERA" is the only source of information about the border crossing by individuals, vehicles and goods (cargo) for departmental automated information systems. The AIS "FRONTIERA" uses the data of the following registers, constituting the information platform (fig. 12):

The State Register of Population, which contains data on individuals and issued documents;
The State register of Legal Units, which includes information on all types of legal units, including their activities, documents and seals;
The State register of Transport, which covers data on vehicles (including numbered units) and registration documents;
The State register of Drivers, which contains data on the right of an individual to drive the corresponding vehicle;
Automated information system Asycuda World monitors the movement of goods on the territory of the country, their transit, as well as the transfer of goods from one customs regime to another one.

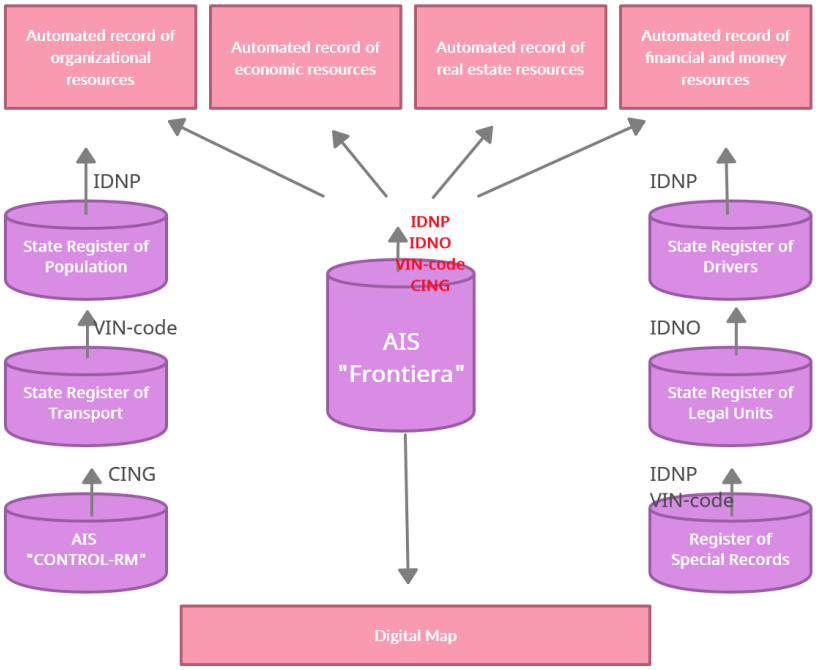


Fig.12. Information platform of the AIS "FRONTIERA"

It should be noted the **registers of special accounting**, which are part of the system of state control over the observance of legislation and financial discipline of the National Information System. They are the tax register and the crime circuit.

The use of identifiers of accounting objects (IDNP, IDNO, VIN, etc.) in all of the abovementioned registers and a single point representation of data makes it possible to obtain integrated data on any accounting object or summary statistical data, if needed. At the same time, separate databases ensure the data protection from unauthorized access.

Therefore, the AIS "FRONTIERA" serves as a source of information about the border crossing for all components of the National Information System.

4.5 Technological space of the AIS "FRONTIERA"

Levels of the AIS "FRONTIERA"

According to the administrative-territorial division of the Republic of Moldova and the organizational structure of the units, participating in the formation of the AIS "FRONTIERA", the system is built in two levels (fig. 13):

- central level;
- local level.

Each of the levels contains one or more information and telecommunication complexes.

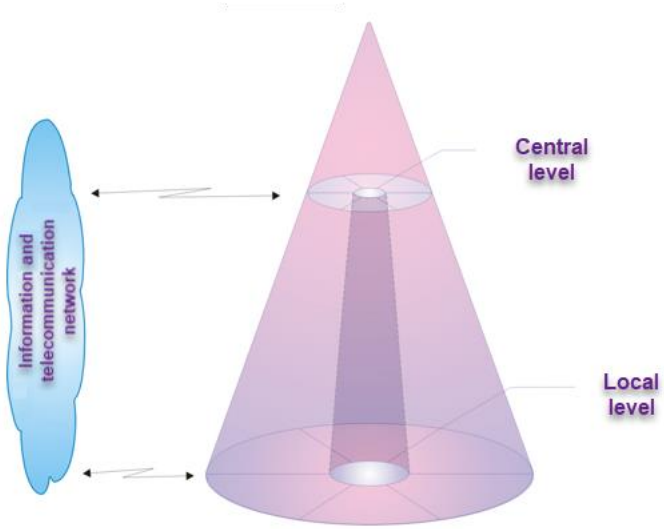


Fig. 13. Levels of the AIS "FRONTIERA"

The territorial location of the information and telecommunication complexes of the central and local levels is shown in fig. 14.

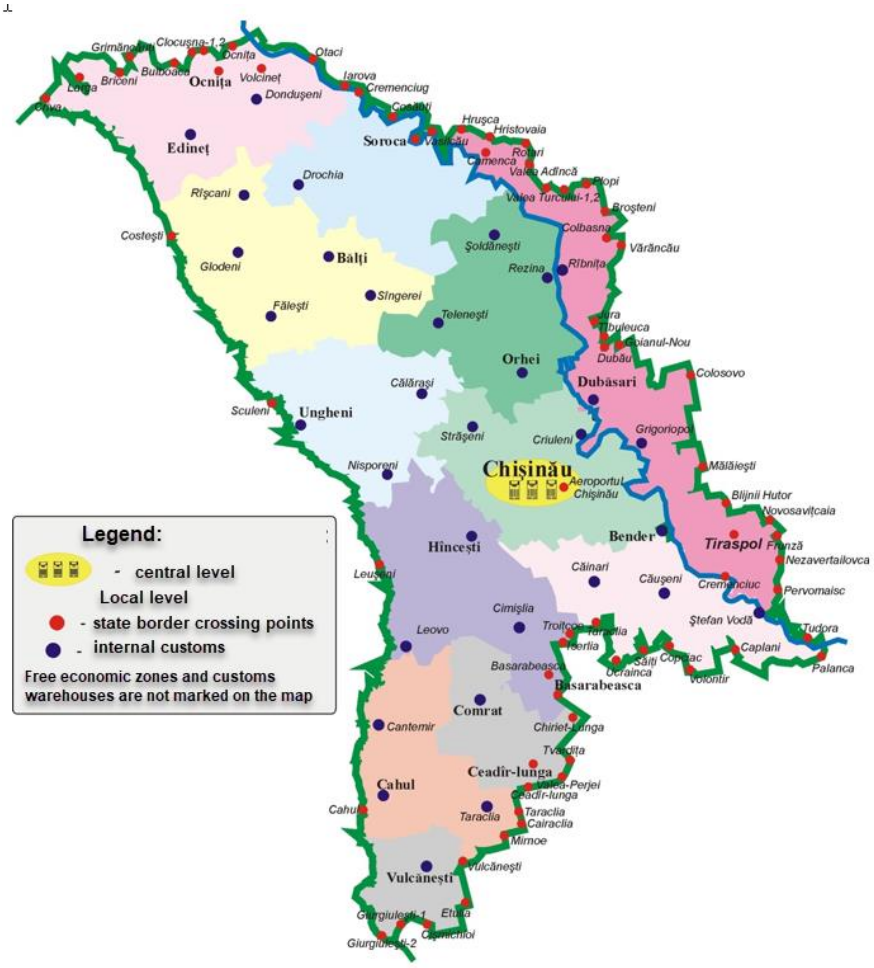


Fig. 14. The territorial location of the information and telecommunication complexes of the AIS "FRONTIERA"

4.5.1 Purpose and structure of the information and telecommunication complex of the central level

The information and telecommunication complex of the central level is located in the municipality of Chisinau and is designed to ensure the functioning of the organizations, involved in the creation and operation of the AIS "FRONTIERA", including the management of the system and the processing of the relevant documents.

The information and telecommunication complex of the central level includes (fig. 15):

- central data bank;
- system administrator automated workstations (AWS);
- system analyst automated workstations;
- local area networks (LAN) of organizations participating in the management of the AIS "FRONTIERA. Each of these networks includes automated workstations for the administrators of the corresponding subsystems and employees of the relevant organizations, as well as local data banks (LDB) with specific service data;
- telecommunication equipment to ensure the connection of workstations and local computer networks with the central data bank, as well as the entire complex with local information and telecommunication complexes.

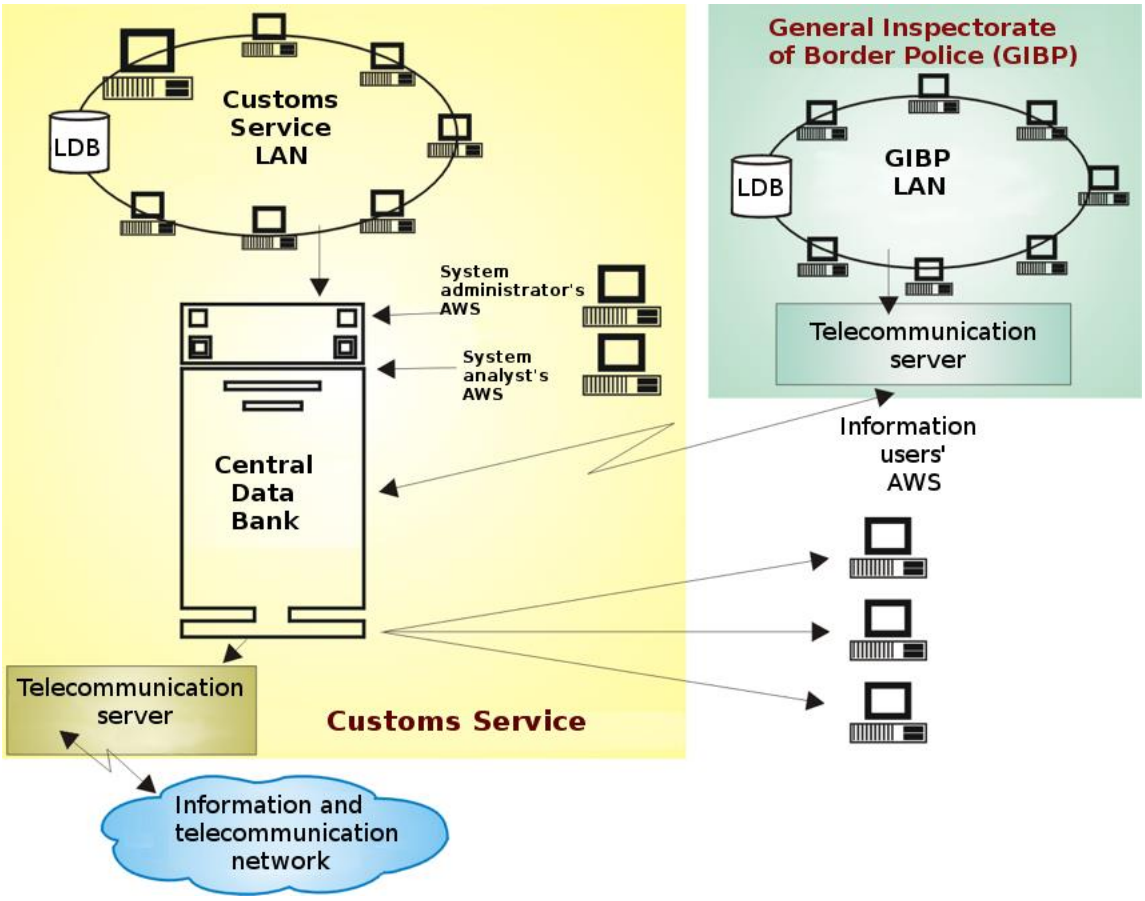


Fig. 15. The information and telecommunication complex of the central level

Several functional modules, that perform specific functions, can be grouped on one workstation, or vice versa, the same functional module can be installed on several similar workstations by the system administrator and the administrators of the corresponding subsystems.

4.5.2 Central database

The central database for storing and processing information, stored in the AIS "FRONTIERA" (fig. 16), consists of the following components:

- data repository is used to collect permanently information about objects of accounting and control and documents, including data on documents, on the basis of which information (forms) about the stages of decision-making and about the dates of decision-making and the names of employees who made these decisions was updated;
- database of formats is designed to ensure security for remote users, and store classifiers and determine the right to access information of a particular user. The connection of users automated workstations with the central data bank is carried out exclusively through the database of formats;
- technological databases are designed for temporary storage of information received from lower levels and requiring a decision by authorized employees, as well as for carrying out all the necessary checks to make a decision. Information from the technological database is stored in the data repository only after the final decision on the form;
- data marts are databases with extracts from the central data repository, designed to provide users with quick and convenient access to the necessary information without

access to the data repository. Data marts can provide certain categories of users with data in the most convenient form (for example, information on export-import operations and their participants is provided to the Main State Tax Inspectorate). Moreover, they are one of the elements of protection against unauthorized access to information, as they contain only the amount of data available to the user. The data updating in marts is carried out automatically when you update information in the data repository.

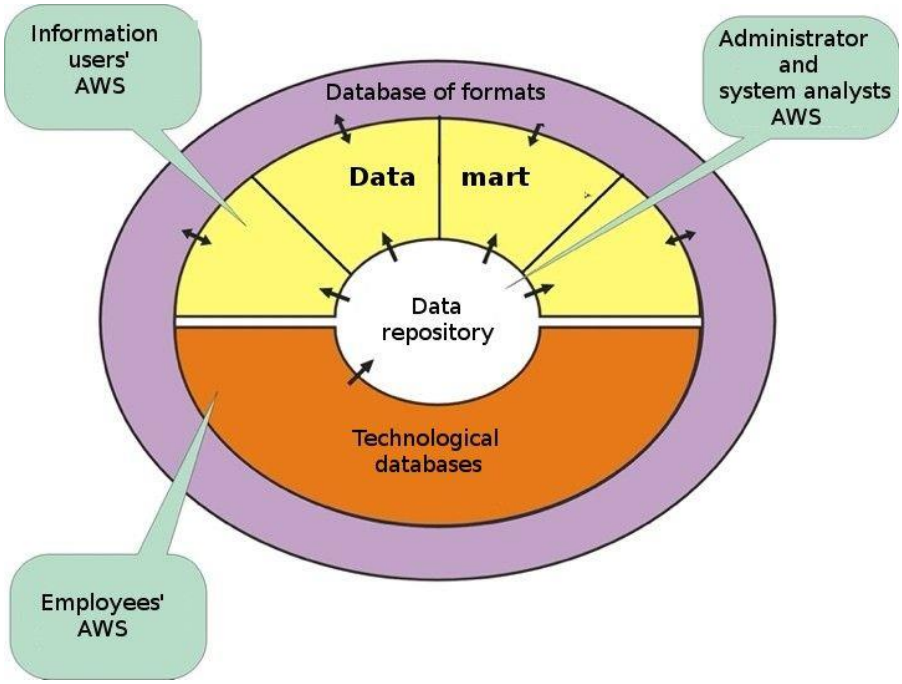


Fig. 16. The structure of the Central Database

Therefore, the AIS "FRONTIERA" uses data marts of other information systems, such as data marts of the State Register of Population, the State Register of Legal Entities and the State Register of Transport.

The exchange of information between the components of the central data bank is carried out through procedures that are inaccessible to external users and are an element of the database protection system.

4.5.3 The structure of the data repository

The data repository includes the following databases:

"Trip" contains data on the consequences of crossing the border, as well as on individuals, legal entities, vehicles and goods (cargo) involved in any way in crossing the border.

"Filter" is designed for storage of filtration arrays. An example of such an array is the list of persons who are prohibited from entering the Republic of Moldova, or the list of wanted vehicles.

5 Non-functional requirements

5.1 Requirements for reliability and fault tolerance

The reliability of the elements of the subsystem should be ensured in the following areas:
- performance of the components of each subsystem;
- data storage.

At the same time, minimal attention should be required from the system administrator in regard of response to elimination of the consequences of module failures, as well as using software and hardware.

The subsystem should provide:
- reliable operation 24/7/365;
- availability to the end users at the minimum level of 99.5%;
- maximum recovery time objective (RTO, no more than 30 minutes);
- maximum recovery point objective (RPO, no more than 2 hours;
- switch to backup power supply automatically within 5 minutes;
- backup power supply (not less than 2 days).

The subsystem should be protected from physical hardware failures by means of logical data recovery and subsystem components using appropriate protocols, containerization and virtualization. A backup system should be created to quickly restore operational configurations from backups in order to protect against errors in system and application software.

The safety of information in case of accidents should be ensured in full. Backups should be provided with the functionality implemented within the system and at the same time by the standard means of the DBMS.

Separate storage facilities (storage) geographically separated from the data center are created to ensure backup of information in case of emergencies. The time spent on restoring the subsystem with technical delays, connecting to the backup data center and monitoring of the functionality should be minimal to ensure continuous operation and should not exceed one hour.

Data preservation should be provided in the following cases:
- power shutdown;
- failure of technical means of information processing;
- errors, crashes, or destruction of software.

5.1.1 Subsystem performance requirements

The capacity of the system elements should be designed to process the corresponding double number of requests.

Preliminary data for calculating the load on the system:

- requests per day: ~ 50000;
- requests per hour (on average) ~ 2000;
- requests per hour (prime-time x4) ~ 8000;
- load requests/hour ~ 16 000 (doubled);
- load requests/sec ~ 4,5 (doubled).

5.2 User interface requirements

It is necessary to provide flexible interfaces for various functionalities and devices, the ability to access the platform from tablets via the web interface.

One of the interface representations at the level of the Monitoring Center of the State Customs Service is an electronic map of Moldova showing the location of all checkpoints.

5.3 Protection of information in the AIS "Frontiera"

5.3.1 Definition of information security system

Information security system means a single set of legal and moral, and ethical standards, organizational (administrative) measures, and software and hardware tools aimed at countering the danger threatening the AIS FRONTIERA to minimize damage to users and information owners.

The main purpose of the AIS "FRONTIERA" information security is to prevent any unauthorized interference in the work, as well as attempts to steal, modify, destroy its components. That is, to protect all system components: hardware, software support and data.

5.3.2 Security threats of the AIS "Frontiera"

The most important aspects of ensuring the security of the AIS "Frontiera" are the identification, analysis and classification of possible threats to the integrity and health of the system.

A threat is a possibility of events, actions, processes or phenomena that may cause damage to system elements.

The most serious types of threats, that were taken into account when creating the security system of the Department of Information Technology, are:

- power, water, heat system accidents;
- faults and failures of hardware;
- consequences of errors in the design and development of system components (hardware, information processing technology, programs, data structures, etc.);
- operational errors (users, operators and others);
- deliberate destructive actions of potential offenders.

5.3.3 General safety requirements

The main principle of accounting is personification, which implies strict observance of the confidentiality of information. When personal data is entered into the AIS "FRONTIERA" database, the work is carried out in the following forms:
- certification and attestation of personal data information subsystems;
- personal data licensing;
- interstate agreements for cross-border transfers of personal information.

The requirements for information security, indicated in the operating documents, ensure safety during installation, setting, operation and repair of technical equipment and comply with current standards and Safety Regulations for the operation of electrical installations

The conceptual model of information security of the AIS "FRONTIERA" is shown in fig. 18.

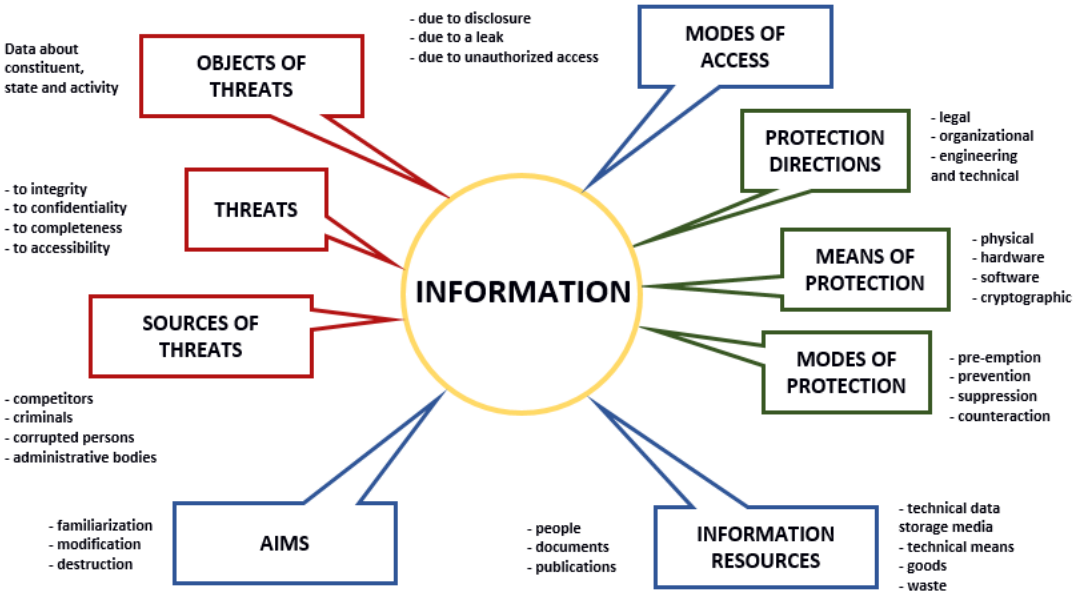


Fig. 18. The conceptual model of information security

5.3.4 Data protection from unauthorized access

The system for data protection from unauthorized access includes organizational measures and software and hardware methods and technical means that ensure blocking:

- data leak through technical means;
- unauthorized access to network resources.

Organizational measures are provided by the relevant services and exclude uncontrolled access of unauthorized persons to the technical means of the information and telecommunication network, magnetic media, hard copies and cable systems.

Hardware and software tools for protecting information from unauthorized access provide:

- identification of protected resources;
- authentication of protected resources and users;
- confidentiality of information circulating in the system;
- authenticated data exchange;
- data integrity when information is generated, transmitted, used and stored;
- permitted access to all system resources under normal operating conditions;

- differentiation of user access to the system;
- differentiation of user access to protected resources;
- management (differentiation of user access to protected resources, processing information from logs, installation and removal of the security system);
- registration of users logging in and out to the system, and access violations to protected resources;
- integrity and performance check of the security system;
- safety in emergency situations.

5.3.5 Data protection in case of accidents

In the case of accidents in the information and telecommunications network, security of information provided by:

- shutdown of individual equipment;
- power outage.

5.3.6 Data protection from external factors

The performance of the technical and software means of the information and telecommunication network is not affected by the electric and magnetic fields in the operating area, possible damages to the power sources and natural disasters.

5.3.7 Information security requirements

The subsystem should be protected from the most common types of attacks, for example, SQL injection, XSS, password brute-force access, etc.

Information that weakens information security (such as session ID, user ID, etc.) should not be publicly displayed.

The following rules should be implemented at the physical level:

- physical access to equipment should be limited and all actions should be recorded (PACS included);
- providing unambiguous identification of users;
- physical access to backups of the subsystem should be limited in accordance with the regulations for the administration of the subsystem and all actions should be recorded;
- ensuring at the network level passing only permitted information flows from the telecommunication networks to the system, as well as in the reverse direction;
- ensuring registration of events related to users' access to system resources (passing/failing authentication), actions of administrators to modify event logs, change settings of software, servers and switching equipment;
- providing the ability to track the history of requests aimed at making changes to the information stored in the databases of the system, and unambiguously identifying users who make such changes (entering, changing, deleting);
- the system should have functionality to limit the number of requests to the database in order to protect it from overload.

Additional information security requirements:

- connection of modules to the local bus, exchange and processing of data should be possible only if the compliance is confirmed in accordance with the established procedure of the integrated information protection system created in it;
- the plug-in should meet the minimum cyber security requirements for its ITS, namely:
- need for regular installation of general software updates (operating systems, database management systems, software libraries, etc.);
- need to control the integrity and authenticity of software updates (both system software and application software, taking into account the peculiarities of the architecture and functioning of the software;
- providing anti-virus protection (protection against malicious code (viruses, trojans, etc.), checking for malicious code of all attachments uploaded by users to the module, blocking the download of executable files and scripts to modules, etc.). If the attachment is damaged by malicious code, it should block the download to prevent its use for illegal and criminal purposes;
- providing appropriate end users guidelines to ensure security of data processed and stored in their information systems (including those deployed using organizational and technical solutions for the deployment of standard components of an integrated information security system).

5.4 Requirements for the development and modernization of system components

Each component of the system should be designed with scalability in mind. All API subsystems should be horizontally scalable. Database servers should be able to scale vertically or horizontally.

5.4.1 Requirements for standardization and unification

Standardization and unification of system functions should be ensured by the use of modern software tools that support a unified design technology and development of functional software.

The software in general, and other software components of the subsystem, should comply with the main international and national agreements and standards in the field of information technology.

For the technical documentation in software development, standards should be applied, but not older than:
- IEEE 830 Software requirements specification and Software Engineering Institute templates;
- IEEE 1016 Software architecture design and Software Engineering Institute templates.

5.4.2 Information software requirements

The information software should meet the following requirements:
- ensuring physical and logical data integrity;
- minimization of redundancy of stored data;
- standardization of data presentation;
- data reliability and relevance.

The system should have properties of an integrated information environment:

- ensure the distribution and assignment of access rights using a role-based or other similar principle;
- provide integration with other information systems using the documented API.

5.4.3 Requirements for types of software

5.4.3.1 Requirements for mathematical software

The mathematical software must include the necessary algorithms for performing data search operations, processing statistical information, and analyzing data.

Information analysis tools should provide quick access to information and have an intuitive interface.

5.4.3.2 Requirements for informational software

Information software created within the subsystem should provide:

- data storage in a form that allows organizing work with the system for many users, as well as automatically restore the system in an emergency;
- distribution and assignment of access rights based on role model;
- real-time access to information resources for system users;
- storage of data on the history of data changes made by users (logging);
- ensuring the integrity of distributed data.
- Informational software the system should meet the following requirements:
- compliance of the database with regulatory requirements;
- use of national classifiers and directories;
- ensuring control over input data processing for correctness of types, spelling correctness in accordance with the existing classifiers and directories, compliance with the established ranges of values, consistency of the data rules;
- ensuring the possibility of working with both structured and unstructured data.

6 Software and hardware complex

6.1 Software and hardware complex of the central level

The software and hardware complex of the central level includes the following components:

- database servers: two 10th generation servers (128 Gb -RAM, 4 Processor – 10 core, storage – 100 GB for operating system and 4 TB for database).
- operating systems: ReadHat Oracle 7.5.
- database management system: Oracle 11.2.0.4.

Automated workstations are based on personal computers with Windows 10 operating system.

6.2 Software and hardware complex at the local level

Information and telecommunication complexes of the local level ensure the functioning of all organizations involved in the management of the system and are located in:

- regional centers (at internal customs);
- border checkpoints (pedestrian and vehicle roads, railways). Checkpoints at river ports and airports are equated to pedestrian, vehicle roads and rail);
- checkpoints across the customs border (customs warehouses, free enterprise zones);

The information and telecommunications complex of the local level includes:
- data mart;
- technological database;
- system administrator automated workstation;
- local area networks of all involved organizations;
- telecommunication equipment to ensure communication of workstations and local computer networks with data marts, as well as the entire complex - with the central information and telecommunications complex (fig. 17).

Fig. 17. Information and telecommunications complex of the local level

Several functional modules that implement specific functions can be grouped on one workstation, or, vice versa, the same functional module can be installed on several similar workstations by the system administrator and administrators of the corresponding subsystems.

The technological database is designed to collect information transmitted to the central level in order to reduce the load on communication channels or in the absence of communication for technical reasons.

6.2.1 A. Software and hardware complex of the local level

Local level automated workstations are based on personal computers with Windows 10 operating system. Automated workstations include specialized equipment for document control and readers for machine-readable documents. Local level automated workstations also include specialized equipment for reading and recording information from electronic chips and related software.

The software for workstations includes various directories, including a directory of identity documents of the countries of the world.

6.3 Administrative infrastructure

6.3.1 Placement of the system

For the development and implementation, the system should be placed in a cloud service. In order to operate the system according to the procedure, the system should have separate environments that are shown in the table below.

Table - List of environments

Environment	Description
PROD	productive environment
UAT	stable environment with the most up-to-date functionality. It can be used to test new functionalities

It was decided that two environments are enough: PROD, UAT.

6.3.2 Backup and disaster recovery system

As part of the development of the system, backup mechanisms, backup and recovery instructions should be provided. Tools for locking configuration files and critical system files (disk images, backup of server operating systems and switching equipment) for their subsequent quick recovery in case of failures should be provided. System recovery includes:
- restoration of configurations of system and application software;
- recovery of users' data;
- data recovery.

6.3.3 Logging system

The system should provide for integration with the central logging modules of the State Customs Service, which provides for the logging of the following events:
- starting/stopping individual services of the subsystem;
- login/logout security events;
- errors in the operation of the subsystem, such as communication errors, data integrity in the subsystem, unpredictable delays in data processing;
- critical events of the monitoring subsystem (critical memory amount, disk space, etc.);
- operation of web services, including audit logging of each request/response of web services;
- other security events.

6.3.4 Automated Testing Systems

All modules of the system should be fully or partially covered with Autotest and unit tests.

The automated testing system was created with the aim of testing new functionalities, emulating an artificial load and reproducing possible errors in a mode as close as possible to real work.

6.3.5 Control and acceptance procedure of the system

A board must be created to accept the system commissioning. It should include representatives of the Customer and the Contractor.

The Contractor transfers the exclusive rights to the developed software to the Customer. If exclusive rights cannot be transferred, the Contractor transfers the rights to the software, providing for the possibility of any modification of the software, by the Customer, or third parties selected by the Customer.

The software must undergo acceptance testing to verify that the system satisfies the technical requirements.

According the results of acceptance tests, an act is drawn up, which contains a conclusion on the degree of compliance of the system with the technical requirements in order to make a decision of its commissioning.

The software must be installed and configured on servers specified by the Customer. The Contractor conducts the acceptance of the system as a whole.

The system must have the following documentation:

1) functional description of the system;
2) data flow diagram + database structure + ER diagram;
3) detailed L2/L3 topology of the system in the form of diagrams;
4) system administrator manual;
5) user manual and their functions;
6) instructions for deployment, update and recovery;
7) transfer and acceptance act;
8) program and test methods;
9) preliminary and other test reports.

6.3.6 Hardware preparation and setting

The Customer shall provide the Contractor with access to the hardware for installing and setting the software package required for the system.

The Customer shall ensure that the Contractor's specialists have access to the above-mentioned tools for final setup and quick software changes.

6.3.7 Personnel training

Training of personnel for operation is performed on the working instance of the system.

Instructing the operators and administrators of the system is carried out by the Contractor by providing the appropriate user manuals and conducting training at the place agreed with the Purchaser.

The number of officials (operators) undergoing training should not be less than 3 people from each territorial body, but not less than 3 people from each department.

Duration of training is up to 5 hours.

Requirements for training system users:
As part of the implementation of the system, training materials should be developed. Training for key users should be conducted on the basis of the developed materials. The training process should cover topics that are necessary and sufficient for users and administrators to perform their functions.

Training scenarios must be prepared before starting training.

The Customer must ensure that key users of the platform implementation are present in the sessions.

Upon completion of the training, the developer must draw up a protocol. All employees, who completed the training, must sign the training protocol.

Annex A: Specific Functional Requirements

N/o	Task	Description
	Systems integrations	
1.	Integration of AIS Frontiera with ANPR&CCTV	Customs Service implements VICOS video monitoring systems within border customs checkpoints. The implementation of these systems involves the installation of intelligent cameras for reading and digitizing the registration plates of transport units, the installation of smart barriers and traffic lights. The implementation of video monitoring implies the need to integrate with the SI of the Customs Service to ensure the automation and fluidization of traffic within the control areas, the exclusion of the human factor from the process of recording transport units in the control areas. Formation of automatic electronic controls for traffic lights and barriers (based on decisions in information systems) regarding permission to enter/exit and move transport units between checkpoints.
2.	Integration of AIS Frontiera with ASP	Currently data on individuals (drivers) crossing the state border automatically comes through the border police. However, there are cases in which the customs inspector is obliged to enter information on individuals in AIS Frontiera who do not participate in the exchange of data with the border police (owner of Transport Unit in case of customs clearance by action, owner of goods within the route etc). In this context, for natural persons resident of RM AND Frontier must ensure the exchange of data with the National Register of Population managed by the PMI. AIS Frontiera will request data from the ASP based on the person's IDNP. ASP will return at least the following data (Name, First Name, Address, date of birth, status).
3.	Integration of AIS Frontiera with ASP Register of legal entities	Currently AIS Frontiera does not have a register of legal entities. Data on legal persons shall be entered manually by customs inspectors on each separate transaction. The register of economic agents of SI Asycuda World cannot be used due to the lack of information requested by AIS Frontiera (lack of transport companies). In this context for legal entities resident of the RM "AIS Frontier" must ensure the exchange of data with the National Register of Enterprises managed by the ASP. AIS Frontiera will request data from ASP based on the company's IDNO. ASP will return at least the following data (Name, Address, Status).
4.	Integration of AIS Frontiera with ASP Transport Units	Currently data on transport units crossing the state border comes automatically through the Border Police. However, there are cases where the data received is incorrectly (manual entry). In this context, it is necessary to verify the data on transport units registered with the National Register of Transport Units within the ASP. AIS Frontiera will request data from ASP based on the registration number of the transport unit. ASP will return at least the following data (VIN code, technical characteristics including UT mass, status).
5.	Change of data exchange with ANSA	Currently the exchange of data with ANTA is one-way in which the customs officer requests confirmation of the validity of transport authorizations. ANTA submits to AIS Frontiera electronic version of the authorization. On the basis of the electronic form, the customs inspector shall receive the decision to allow the transport unit to leave the Customs Control Zone. This is a risk of exceeding the number of transactions allowed by the authorization or failure to comply with the conditions of use of the authorization. It is therefore requested for each transaction registered under the AIS Frontiera on transport authorizations to transmit the information on

		the transaction to the ANTA address (authorization number, country of departure, country of destination, country of registration, etc.). Thus ANTA will verify the data and take records of the transport authorizations used. ANTA will deliver to "AIS Frontier" the result of the control (Accept/Refuse, reason for refusal) As a consequence, the responsibility for the permission of the transaction under the authorization remains with ANSA.
6.	Integration with Anti-fraud	Ensuring the synchronization of the blacklists of the AIS Frontiera with the lists of persons, economic agents and transport units who have committed crimes or have been detected at increased risk of committing crimes within the SI Anti-Fraud. Delivery of information from AIS Frontiera in IS Antifraud on the results of checks of nominated persons and transport units.
7.	Integration with Border Guard Service	Currently the passenger individuals of the transport unit crossing the state border are not subject to the exchange of data between the "AIS Frontier" and the SI of the Border Guard. The following data exchange mechanism with the Border Police is therefore requested. SI Anti-Fraud forms a risk profile and transmits it to the SI address of the Border Guard. The Border Guard confirms its reception. If the IS of the Border Police detects the presence in the control area of the person concerned, the IS of the Border Guard transmits that information to the address AIS Frontiera (information about the person, information about the risk profile).
Changes to user interface		
8.	Adding ANSA user interface	The initial ANSA interface was designed as part of the interface at the customs checkpoint. Currently ANSA inspectors are present in customs control areas and de facto are not included in information flows within customs control zones. Thus the calculated payments are not included in the single payment voucher and the ANSA controls are not even reflected in the information systems (control time, control result, etc.). Therefore the control of ANSA makes the use of VICOS in customs posts virtually useless. The ANSA interface shall ensure that ANSA users can indicate the results of the control and the inclusion of the calculated payments in the single payment voucher. The ANSA interface does not automate ANSA's internal processes.
9.	Adding Warehouse user interface	Currently the representatives of the customs warehouses (CTIF officials) do not have access to SI Frontiera. Payments for services within the warehouses are not included in the single payment voucher. The working interface for users of customs warehouses shall contain the following information: • Description of the service provided (classifier) • Date of start of service • Service Finish Date • Amount of provided Service • How to pay for the service provided Services that require cash payment will be included in the single payment voucher, the wired payments for services.
10.	Change to Scan interface	In addition to the existing data in the AIS Frontiera the interface must provide for the possibility of adding graphic images (the result of the scan). For suspicious cases the attachment of the image must be mandatory. The format of the graphics files and the attachment mode will be determined by the developer in common with the

		responsible persons of the Customs Service at the business analysis stage of the process.
11.	Adding Entry/Exit interface	Currently the transaction is initiated by the Border Police or at the customs checkpoint. With the implementation of the VICOS system, there is a need to automate checkpoints at entry/exit barriers in/out of customs control areas. Since the entry/exit control point in/out of the control area in the direction of exit from the Republic of Moldova and the entry/exit control point in/out of the control area in the direction of entry into the Republic of Moldova are managed by a person in each direction, the interface must combine the entry/exit control points in/from the customs control zone. The input/output interface must therefore contain two distinct zones. • Entry to the control area • Exit the control area The entry area must ensure the possibility of registering the new transaction, i.e. the user must enter the following data into the system: • Automatic system operation ("Control Zone Entry") • The direction (RM/RM Output) automatic system depending on the configuration of the checkpoint • Registration number (tractor head/trailer) • Date and time of automatic system transaction registration Confirmation of the transaction registration under the "AIS Frontier" will automatically activate the entry barrier (if applicable). If the checkpoint is connected to the ANPR&CCTV system the registration number will be automatically filled in by the system. In this case the user must confirm the accuracy of the reading of the registration number. If the ANPR&CCTV system could not read the registration number or interpretit it incorrectly, the user must correct the registration number. And with the registration of the transaction AIS Frontiera will submit to the address of the system ANPR&CCTV information on the corrected number. The exit area shall ensure that the exit from the customs control zone is confirmed, i.e. the 'AIS Frontiera' shall make available to the user the list of transport units for which exit from the control zone is permitted in the direction of the control point. The user must confirm the exit of the transport unit to the barrier. After confirmation of exit (closing of the transaction) "AIS Frontier" will automatically activate the exit barrier (if applicable). If the checkpoint is connected to the ANPR&CCTV system the decision to close the transaction will be taken automatically by the system. If the ANPR&CCTV system could not read the registration number or interpret it incorrectly, the user must correct the registration number. And with the registration of the transaction AIS Frontiera will submit to the address of the system ANPR&CCTV information on the corrected number.
12.	Adding VICOS tab to access ANPR&CCTV	Depending on the configuration of the checkpoints, for cases where the checkpoint is connected to the ANPR&CCTV system, the AIS Frontiera will present the VICOS TAB to users. The TAB will contain the graphic information (images, video) assigned to the transport unit when it is verified. In cases where the ANPR&CCTV system could not link the transaction to the graphic information, AIS Frontiera will force the user to assign the graphic images manually to the transaction. In this case "AIS Frontier" will make available to the user the list of images and videos that have not

		been assigned to any transaction. The user will select one or more images/video and attach them to the transaction. If the checkpoint is connected via the VICOS system to the barrier and (or) traffic light, the AIS Frontiera will provide the user (via the TAB) with the manual control of the barrier and/or traffic light.
Other functionalities		
13.	Return	The return functionality will be made available to the user at the customs checkpoint for the shift manager and the local administrator. The option can be used for all active transactions regardless of whether the checks have been completed or not. The transaction will be directed to the exit checkpoint from the direction through which the transaction was recorded. With the selection of the return operation the system user must correct at least the following data: • Date and time of operation (automatic system) • Data about the user who performed the return operation (system automatic) • Reason for return (classifier) • Comments on return operation (free text)
14.	Unloading in customs control zone	Currently AIS "Frontiera" does not carry the record of goods kept in the territory of the customs control zone (without customs clearance procedure). In practice it often happens when for various reasons carriers are not able to introduce or remove in/out of the country certain categories of goods (lack of documents, lack of financial means for customs clearance, etc.). In this case AIS "Frontiera" will give the user at the customs checkpoint the possibility to record the fact of unloading (keeping) the goods in the customs control area. At least the following data will be recorded to register the download operation in the "AIS Frontiera": • Transaction Identifier • Download Operation Identifier • Date and time of operation (automatic system) • Data about the user who performed the download operation (system automatic) • Reason for unloading (preservation) (classifier) • Comments on download operation (free text) • Place of storage • Commodity code (4-10 characters) • Description of the goods • Quantity • Weight • Value AIS "Frontiera" will allow the registration of several goods as appropriate.
15.	Loading in customs control zone	AIS "Frontiera" will allow the collection of goods kept in the customs control zone by two possibilities: • Self movement • Loading goods to another transport unit In the case of Self-movement – the user at the customs checkpoint initiates a new transaction and determines the direction of exit. After initiating the transaction the flow will continue as a standard transaction processing stream.

		In case of loading of goods to another transport unit the user from the customs control point will attach the data about the goods to the transaction open to the transport unit in question and will determine the direction of exit. The processing flow will continue as a standard transaction processing stream. In this context AIS Frontiera will give the user within the customs checkpoint the possibility to select from the list of goods kept in the customs control area of the goods that will be removed by recording the following data in the system: • Previous transaction identifier (automatically from the register of kept goods) • Current Transaction Identifier (System Automatic) • Identifier of the unloading operation (automatically from the register of preserved goods) • Date and time of operation (automatic system) • Data about the user who performed the download operation (system automatic) • Reason for loading (preservation) (classifier) • Comments on the boot operation (free text) • Commodity code (4-10 characters) (automatically from the register of kept goods) • Description of the goods (automatically from the register of kept goods) • Quantity (user manual in case of partial and automatic system loading in case of total load) • Weight (user manual in case of partial and automatic system loading in case of total loading) • Value (user manual in case of partial and automatic system loading in case of total load) The AIS Frontiera will allow the partial loading of goods to be recorded as appropriate. In the case of partial loading AIS Frontiera will manage the stocks of goods kept in the customs control area.
16.	Transaction update	Access to transaction change will be assigned to the local administrator and the central administrator. The functionality will allow the user to modify any data for all checkpoints within the customs post. AIS Frontiera will ensure that the transaction is maintained until the transaction is changed as a transaction history. To register the AIS Frontiera change, the user will request the user to enter at least the following data: • Date and time of change (automatically) • User data (automatic) • Reason for change (classifier) • Comments (free text)
17.	Transaction cancelation	Access to cancellation of transactions will be assigned to the local administrator and the central administrator. The functionality will allow the user to cancel the transaction in full. AIS Frontiera will ensure the preservation of the transaction and mark it with the indicator "Cancelled". To register the cancellation AIS Frontiera will require the user to enter at least the following data: • Date and time of cancellation (automatic) • User data (automatic) • Reason for cancellation (classifier) • Comments (free text)

Administration		
18.	User management	Currently user management is ensured by system developers. There is no distribution of roles on control tracks and other user management elements (active or free shift, etc.). These discrepancies are due to the initial burden of the system in which all control points were replaced by a single customs checkpoint. Therefore, the correct user management enforcement AIS Frontiera will ensure the following functionality: • The registration of local-level administrators will be allowed exclusively to central administrators. • Registration of users at the checkpoint level will be allowed to local administrators and administrators at the central level. • Designation of users on check tracks and assignment at checkpoints will be allowed to shift managers, local administrators and administrators at the central level. To register users within the system, the administrator must enter at least the following data. • Date and time of registration (automatic) • Data about the person who made the record (automatically) • IDNP of the person (manual) • Name, first name (web-service ASP) • Function (manual) • Authority of the name of which the registered person is (Classifier) • Customs post at which registration takes place (classifier) • User role (classifier) • Administration indicator (indicated for management of customs posts, shift heads and administrators) • Status of the person • Contact date • email After the user registers by the administrator, the system will assign the created user the status "Pending confirmation". After registration the user will receive a link via email through which he will be able to continue registering (will establish username and password). After completing the recording, the system will assign it the status "Active". AIS Frontiera will contain at least the following roles: • Administrator central level • Customs service • Administrator central level • Management of the customs post • Head of shift • CP Entry RM • CP Customs • CP ANSA • CP Scale • CP Scanner • CP Warehouse • CP Exit RM The list of authorities shall contain at least the following agencies: • Border Police • Customs Service • ANSA • CTIF

		Users without the "Administration" indicator will not have access to the operations within the station until the shift manager assigns the track and checkpoint to the user during the shift. For the distribution of users during the shift, AIS Frontiera will provide the shift manager with an interface in which the list of checkpoints will be viewed in accordance with the configuration of the customs post. When selecting the checkpoint the system will view the list of persons with access to the respective checkpoint. The assigned shift leader for each user ticks the following indicators: • It's on shift (yes/no) • Direction (RM entry or/and RM exit) if the control point provides • Track (goods or/and passengers or/and CD or/and Coach) if the checkpoint provides After setting the shift by the shift manager all users with "It's on shift" will have access to transaction lists at the nominated checkpoints. The user management system must ensure good practice in user information security (password encryption, password compliance check, password modification request). AIS Frontiera must allow authorization in the system with digital signatures.
19.	Checkpoints configuration	Current functionality is missing within SI Frontier. The configuration of checkpoints is done by developers at the source code level. The configuration of customs checkpoints is an extremely important functionality due to the large diversity of checkpoints starting with the types of customs checkpoints (rail, road, air, checkpoints at the administrative perimeter with Transnistria) the size of the checkpoints (including the common entrance/exit runway) Equipment of checkpoints (no scale, with a scale with several scales, etc.), with the presence of other agencies or the exclusive presence of the Customs Service. In this context AIS Frontiera must assure the administrators at central level with the possibility of setting up each separate customs post. The checkpoint configuration interface must require the user to enter the following data: • Customs checkpoint code (Asycuda Classifier) • Name of customs post (Asycuda Classifier) • Code of the country where the post is located (Asycuda Classifier) • Type of customs post (road/aeriam/rail/fluvial) • Number of inbound tracks (manual) • Number of Exits Tracks (manual) • List of checkpoints and their name (classification control points) • Configure the checkpoint (set of parameters) The list of checkpoints shall contain at least the following values: • CP Entry RM • CP Customs • CP ANSA • CP Scale • CP Scanner • CP Warehouse • CP Exit RM When selecting the checkpoint, the administrator can establish a description of the control point. The system will allow duplication of the checkpoints. Checkpoint configuration parameters will contain at least the following values: • Connected to ANPR (yes/no)

		• Connected to traffic light (yes/no) • Connected to the barrier (yes/no) • Direction (entry or/and exit) • Mode (passengers or/and cargo or/and CD or/and Coach) • Runway assignment (track number) • Location sequence (no track direction order) • Mandatory checks (yes/no) • % Checks progress (0-100) • Random distribution (yes/no) The result of the configuration of the customs checkpoint will serve the AIS Frontiera reconfiguration of business processes within the customs checkpoint and will provide a direct impact on the user management system.
20.	Logging system	All activities of AIS Frontiera users must be recorded in logs so that: • authentication (entry and exit) of users, successful and unsuccessful authentications attempts; • Creating, copying, moving, deleting, modifying local accounts and configuration files. • failed or rejected user actions. • user who has access to access objects. The Log must contain the following fields: • date and time • event source name (service/service) • account name / user ID; • customer's IP address; • the start time of the operation; • the end time of the operation; • event level (determined by operator); • event category (determined by Operator); • description of the event. AIS Frontiera must provide administrators with tools for viewing and filtering data from log. "AIS Frontier" shall provide administrators with tools for obtaining statistical data from LOG logs. For records in LOG logs, special access regime must be provided – for the System Administrator (for viewing), as well as for the Information Security officers. All actions of System Administrators are also recorded in the Log logs of SI Frontiera.

Annex B: Institutional Arrangements

The Service Provider will work under the guidance of the IOM Project Coordinator for substantive aspects of the assignment and under the direct supervision of the IOM Procurement Focal Point for administrative aspects.

The Service Provider is expected to cooperate closely with the representatives of the Customs Service of the Republic of Moldova, General Inspectorate of Border Police, E-Government Agency, other public authorities engaged in AIS "FRONTIERA" as well as with IOM technical experts.

All the deliverables shall be submitted in English and Romanian language, in hard copy and/or electronic format. All other documentation related to the assignment shall be in Romanian. All documents submitted, in English and Romanian, will be subject to proofreading and editing to ensure compliance with the language and terminology in the national legislation regulating the subject matter of the assignment.

Before submission of final deliverables, the Service Provider will discuss the draft documents with the parties involved, so that the final products reflect their comments. All the deliverables of the Service Provider shall be coordinated with the IOM Project team.

The bidder will provide support facilities to their team of experts (back-stopping) during the implementation of the contract.

Bidders agree that experts will provide high quality outputs and expertise and participate in the project at the level and duration specified. Should any changes be necessary in this regard, a formal request for the agreement of IOM Project coordinator to allow substitutions, shall be submitted.

During the assignment, the Service Provider's team of experts should prove commitment to the core values of the United Nations, in particular, respecting differences of culture, gender, religion, ethnicity, nationality, language, age, HIV status, disability, or other status.

Annex C: Minimum Eligibility and Qualification Criteria

The bidder shall provide documentary evidence that it meets the following financial requirements:

The average annual turnover of the Bidder should be not less than **USD 350,000.00** (three hundred fifty thousand), or equivalent, for the most recent three (3) years (2018, 2019, 2020) and this turnover must have been derived solely through the provision of Information Technology (IT) Systems and services.

The Bidder should provide audited financial statements and balance sheets for the last three complete financial years demonstrating the soundness of the Bidder's financial position and demonstrating that it has the financial resources necessary to handle the requirements of the proposed Contract.

Experience and technical capacity:

The bidder shall furnish documentary evidence (including information about the completed contracts and contact information of clients from whom the references could be taken or whom the Purchaser may, when necessary, visit to familiarize themselves with the systems put into operation by the Bidder) to demonstrate that it meets the following experience requirements:

It should have been in operation for at least 5 years with an important part of its business being the provision of Information Technology (IT) Systems, including software and services.

The successfully completed similar contracts shall be documented by a copy of an Operational acceptance certificate (or equivalent documentation satisfactory to the Purchaser) issued by the purchaser(s).

Annex D: Project Team Requirements

In the technical offer, the Provider will present the data regarding the personnel involved in the project and their qualification. The involvement of qualified personnel with experience in the development and implementation of informational systems with similar complexity for border and customs authorities of Moldova is welcomed.

For all team members, knowledge of the English language is required, and knowledge of Romanian and/or Russian is an advantage. Due to the complexity of the task and increased workload, the bidder is asked to provide 4 (four) Full Stack Software Developers.

The following core team of experts shall be proposed by the Bidder:

1	**Project Manager:**
	University degree in Management, Engineering, ITC or another relevant field
	At least 10 (ten) years of professional experience in the field of design, development and implementation of complex software solutions
	At least 3 (three) similar successfully completed ICT projects with similar complexity, in a leading role throughout the entire duration, proven by brief descriptions of project scope and outcome, and proofs of completion
	Experience in the development of software for border/customs authorities would be an advantage
	Proved certification in Project Management
	Proficiency in Romanian, Russian and English language
2	**Software Architect:**
	University degree in the field of Computer Science and/or Information Technologies
	At least 10 (ten) years of proven track record of designing enterprise systems
	Docker and Kubernetes Certifications is a strong advantage
	Proven track record of designing and successfully implementing projects for the Government of Moldova. Experience with MCloud integration is a strong advantage.
	Proficiency in English language. Knowledge of Romanian or Russian is an asset
3	**Senior Technical Lead**
	University degree in the field of Computer Science and/or Information Technologies
	At least 5 (five) years of experience developing projects of similar complexity
	Proven track record of designing and successfully implemented projects for the Government of Moldova
	Strong experience and knowledge in MCloud, Java, Docker, Kubernetes, Microservices, Apache Kafka, JavaScript, React
	Fluency in English. Knowledge of Romanian or Russian is an asset
4	**Senior Full Stack Software Developer**
	University degree in the field of Computer Science and/or Information Technologies
	At least 3 (three) years of experience developing projects of similar complexity
	Experience with MCloud, Java, Docker, Kubernetes, Microservices, Apache Kafka, JavaScript, React
	Fluency in English. Knowledge of Romanian or Russian is an asset
5	**Database Developer**
	Master's degree in the field of Computer Science and/or Information Technologies
	At least 3 (three) years of experience of developing/maintaining databases of similar complexity
	Oracle professional certification
	Fluency in English. Knowledge of Romanian or Russian is an asset

Annex E: Stages of software modernization and indicative timeframes

The Action Plan intended to complete the assignment is displayed below. Pursuant to the Action Plan, the deadlines for carrying out the Project activities are as follows:

No.	Action	Proposed Timeframe
1.	**Inception phase**	*1 Month*
	1) Preparation of a detailed work plan, presentation of the project management system, communication plan for the provision of intermediate and main work results. Approval of the Plan by IOM and the beneficiary. 2) "Terms of Reference" update and it's presentation in electronic and hard format. Updated ToR will meet state standards for software and ITS documentation, agreed with IOM and the beneficiary, and which should contain an agreed list of technical documentation to be provided after the system upgrade. The detailed TOR will also include requirements for the equipment (servers and hardware infrastructure) on which the software will be installed.	
2.	**Phase II**	*3 Months*
	1) Demonstration of functionality responsible for the implementation of key business processes and the administration subsystem, except for functionality responsible for integration with other systems. 2) Provision of documentation in paper and electronic form, containing test plan, test cases, system testing protocol, preliminary user instructions. 3) Approval of the IOM system testing protocol by the beneficiary.	
3.	**Phase III**	*2 Months*
	1) Demonstration of functionality responsible for integration with other systems. Providing documentation in paper and electronic form, containing a description of the rules of delimitation of user access, the parameters of integration with other systems. 2) Approval of the IOM system testing protocol by the beneficiary.	
4.	**Phase IV**	*1 Month*
	1) Installation of a modernized information system on the productive environment of the beneficiary 2) Testing the updated system. Functional testing. Performance and safety testing. 3) Training of selected users. The training requirements are described in paragraph 6.3.7 of the present TOR.	

	4) Final acceptance and commissioning of the system. Commissioning of the system begins with the signing of the act of commissioning of the IT system and the beginning of its operation.	
5	**Maintenance Support Phase**	*12 months*
	During this period, the provider will deliver technical support to correct any shortcomings related to the functioning of the System and assist the beneficiary of the system in maintaining the capacity of the IT system to provide services, as well as the modification of the product (elimination of errors, optimization of the operating parameters, installing and integrating amendments), preserving its integrity. The service provider also will ensure the transfer of additional knowledge if it is deemed necessary by the beneficiary staff in the technical support period. Additionally, the contractor will provide any available updates and upgrades to the installed IT solution, including DBMS, and other software components.	
6	**Warranty Support**	*36 months*
	During this period, the provider assumes the obligation towards the beneficiary to assist in troubleshooting of problems related to the development/configuration of the IS functionalities not identified during testing and acceptance phases in a warranty period.	

Overall, approximately 7 calendar months would be required to ensure the developments, 36 calendar months for warranty support and 12 moths for and maintenance support services.