Modernization of Government Services Project
in the Republic of Moldova

Credit no. 6126-MD / Loan no.8774-MD

Contract No. MD-EGA-268046-CS-QCBS

Terms of Reference

for design, development, and deployment
of the information system of National House of Social Insurance
(NHSI) of the Republic of Moldova

1. Contents

2. General

2.1. Background

The Government of Moldova is determined to fundamentally change the way how public services are provided in Moldova through a variety of interventions for modernization of service delivery, which combat corruption, foster a customer care culture, enhance access, as well as increases efficiency in the Moldovan public administration.

Therefore, one of the main objectives of the Administration Reform Strategy 2016-2020 and Government's activity program is the modernization of public services.

The Government has launched the reform of public services in 2014-2016 and has committed to digitize and provide online access to all public services by 2020, re-engineering and process optimization remains a problem that prevents achieving this.

Also, there is room for rationalization to circa 688 existing public services by eliminating obsolete services.

The Government of Moldova, via e-Governance Agency as implementing agency is carrying out a World Bank-funded PAR operation, planned for 2017-2023 - Modernization of Government Services Project – (MGSP) as part of which circa 85 services have undergone reengineering and are currently on various stages of digitalization.

Major expected results of the project include better quality, accessibility, and increased efficiency of selected governmental administrative services through the public service modernization and creation of digital platforms and services.

This document represents requirements for the modernisation and/or replacement of the existing "Social Protection" information system of National House of Social Insurance (NHSI) of the Republic of Moldova.

The "Social Protection" IS is a part of the state information systems and is a set of interconnected information resources and technologies, technical means of programming and methodologies, designed to keep track of payers and social insurance contributions to the state social insurance budget, to establish and keep track of the payment of pensions and social benefits and to manage the state social insurance budget.

Requirements presented herein are based on the target (TO BE) model of reengineered public services, provided by the NHSI.

2.2. Definitions

The following definitions, abbreviations and acronyms are used throughout the document should in the particular case is not stated otherwise.

Agile

Agile software development is a set of practices to enable iterative software development process by dividing whole development project into a set of small activity sets. Thus, each activity set brings to the client a piece of functionality ready to assess, test and/or use. In this document we engage SCRUM as one of agile project management methodologies.

API

Application Programming Interface.

Beneficiary

National House of Social Insurance of the Republic of Moldova will be the final beneficiary of the developed system and will actively participate in the process of the system development and implementation.

BPM

Business Process Management.

BPMS

Business Process Management System — an information system that automates business processes.

Client

e-Governance Agency will be responsible for all financial and organizational activities related to the Client responsibilities.

Consultant

The company that according to contract will provide IS development, developed IS implementation and deployment, as well as accompanying activities like analytical tasks, documenting, training, data migration etc.

DB

Database.

DTS

Detailed technical documentation, created by Consultant, that contains detailed description of IS technical implementation.

EGA

e-Governance Agency.

GB

Gigabyte.

ICT

Information and communications technology.

IDNO

Unique identifier of legal entity in Moldova.

IDNP

Unique identifier of natural person in Moldova.

IS

Information System.

MB

Megabyte.

MCloud

The MCloud platform is a common government information infrastructure that operates on the basis of cloud computing technology hosted in the consolidated data centre infrastructure.

MConnect

Moldova's governmental system interoperability platform, the technological solution developed by the Government of the Republic of Moldova to ensure interoperability and data exchange between information systems.

MPass

Moldova's governmental single authentication and access control service. Ensures single sign-on and other related functionality.

MPower

A reusable government service that aims to provide a secure, flexible and convenient mechanism for managing the authorization registries of individuals and legal entities.

MSign

Integrated governmental service of the electronic signature.

MLog

Governmental service for activities logging

MNotify

Governmental electronic notification service that allows service providers, authorities and public institutions (Sender) to send notifications to users (Recipients) for notification, of events produced in connection with the provision of services or other relevant events to recipients.

NHSI

National House of Social Insurance of the Republic of Moldova.

Product

In general, includes as developed information system as results of all accompanying activities like documentation, manuals, etc.

PAR

Public Administration Reform.

PSA

Public Services Agency of the Republic of Moldova.

RM

Republic of Moldova.

SFS

State Fiscal Service

SRP

State Registry of Population

SRLE

State Registry of Legal Entities

UI

User interface, a part of IS intended for interaction between the human user and the system.

WB

World Bank.

WP

IS user workplace.

3. Project implementation approach

The scope of work is to design, develop, configure, and implement the information system as a fully functional product with all functionalities in place, according to the specifications iteratively identified and defined by the client (the indicative set of requirements is listed in sections 0“Software requirements specification (SRS)” and 4. “Annexes” below) and following the development approach described below.

The development of the solution will follow Agile iterative software development principles. Since there are many dialects of agile software development and to avoid misunderstandings, this section provides key principles to be used in development of the solution.

3.1. Iterative development

In contrast to waterfall software development approach, the solution shall be developed in iterations named sprints. This means that the implementation of different functionalities will take place in phases with some modules being in production while others still being in development. The priorities of functionalities included in a sprint will be determined by the client. Sprint duration will be determined by the client together with the Consultant. Consultant will propose the overall system architecture so the planned functionalities should completely by covered by this architecture with all workflow data sources.

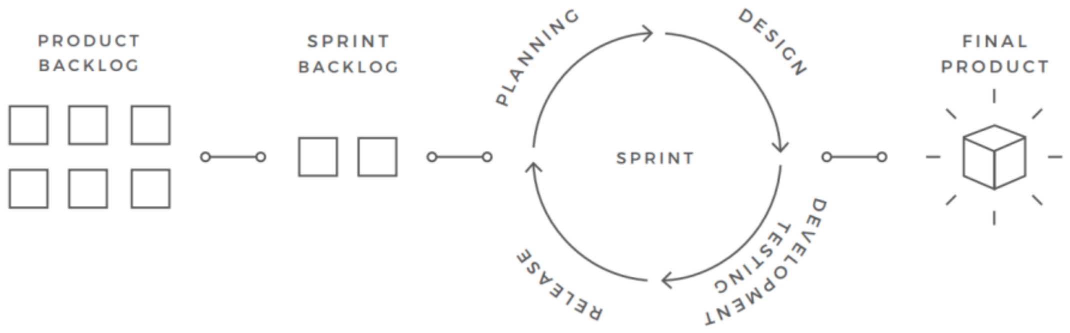
3.2. Agile development

The development shall follow agile principles by allowing change and flexibility in implementation. Client will maintain the master list of generic requirements for the solution– product backlog, which consists of ordered business and technical requirements as seen by the client. Items in product backlog are ordered by the client by their priorities. Client is free to manage the product backlog by adding new items to it, removing items and reordering them as he/she desires. At the beginning of each sprint, the topmost N items that fit into a sprint are taken, and a sprint backlog is built out of them. Items in sprint backlog are further detailed and distributed to developers. Sprint backlog is not changed during the sprint.

Overall agile development cycle is presented in picture[1] below:

[1] Picture source: https://dihfahsih.blogspot.com/2019/07/documentation-is-very-vital-before-you.html

Agile Development Cycle



3.3. Working product in each iteration

Each sprint ends up in a working product which is presented to the client for acceptance in the last day(s) of sprint. The working product shall meet the agreed readiness criteria (i.e., it must be fully functional, fully tested, accompanied with relevant unit tests, accompanied with relevant documentation where necessary, complete commented source code supplied etc.). In case the deliverables contain defects for reasons not imputable to the client, the Consultant shall fix them without impacting the time schedule and at no additional costs, including possible visits to client site. Working products from different sprints can be combined into a release deployed in production at client's discretion. Any incidents reported by the client after the release, shall be solved by the Consultant according to the agreed Service Level Agreements (SLAs) as defined in section 4.1.5. "Warranty and Support".

To ensure that the development team is in position to deliver on time working products, a client representative – typically named the Product Owner in agile methodologies – will be permanently available to the team for answering eventual questions, thus not slowing down the implementation pace.

The Consultant will appoint a Scrum Master from the team of key or non-key experts for the entire duration of the project.

The Scrum Master will be responsible for the day-to-day liaison with the client; she/he must ensure the internal coordination and guidance of the project experts and the project coordination with external counterparts.

The Scrum Master must also ensure the availability of suitable experts in accordance with the project planning documentation.

3.4. Reporting Requirements

The following reports will be provided during the assignment:

a) Sprint Report, including release notes, breakdown and duration of tasks implemented during the sprint, velocity, issues and outstanding problems, proposed actions to be taken;

b) Next Sprint Backlog, including breakdown and estimated duration of tasks proposed to be implemented during the next sprint, resources that are expected to be provided by the Client and/or actions to be taken by the Client;

c) Training reports, submitted after each training session, including:

- Participants list;
- Training session agenda;
- Training materials (presentations, labs etc.);
- Trainees' test results;

3.5. Client involvement

In contrast with commonly used waterfall model for procurement and implementation of information systems for the government, the client designated person – Product Owner – will be heavily involved in the development process. The Product Owner will have three core responsibilities:

- Maintenance of product backlog – the Product Owner will maintain the product backlog up to date, so it reflects prioritized list of desired functionalities.
- Answering to questions coming from developers – the Product Owner will be at all time available to the development team for answering their eventual clarification questions, thus avoiding complex and formal communication within the project. This is essential to ensure the team has all the information on time to deliver a working product at the end of the sprint.
- Acceptance of working packages – delivered working packages are presented to the client for acceptance at the end of each sprint. The client shall accept the working package or notify the Consultant of any defects during the following sprint.

Although it is not strictly necessary, the Product Owner may participate in team stand up meetings listening for progress and eventual blockers for an immediate reaction.

Product Owner also decides on product releases, as per release plan.

Also, as per the principles of agile project management methodology, the client will define the Product Vision Statement and Product Roadmap in order to track progress and to ensure the appropriate product development.

3.6. Recommended technology stack

To preserve e-Government investments, the solution is recommended to be developed using the latest versions of the following technology stack:

- Programming language is C#.
- ORM is Entity Framework Core.
- Web framework is ASP.NET MVC Core.
- RDBMS is SQL Server.
- Container engine is Docker.
- Container orchestration is Kubernetes.
- Cache server and session store is SQL Server or Redis.

During the development process, the Consultant or the Client may propose use of additional components required for the development and proper functionality of the solution in production. Upon the Client's approval of such components, the costs for them shall be added through amendments to the contract.

During the project implementation E-Governance Agency will offer the development environment that includes:

1) Supervised Azure subscription with AKS and other PaaS services in-cluster and out-of-cluster (such as SQL Server) as required by the project with required access rights assigned
2) Supervised Azure DevOps organization associated with the subscription and Consultant users invited as guest with required access rights assigned
3) Connectivity from Azure to on-prem services involved in the project
4) Access to on-prem Kubernetes cluster(s) for production deployment

3.7. Consultant's requirements

The Consultant shall furnish documentary evidence (including information about the completed contracts and contact information of clients from whom the references could be taken) to demonstrate that it and its key experts meet at least the experience requirements listed below.

3.7.1. The Consultant Qualifications

The Consultant minimum qualifications requirements are:

- Minimum 5 years of experience in developing ICT solutions/systems.
- Minimum 3 ICT projects of similar complexity successfully implemented during the last 5 years.
- Experience developing ICT solutions/systems for State/Public Institutions (Central and/or Local) *will constitute a strong advantage*.
- Experience developing ICT solutions/systems for company/corporate registries *will constitute a strong advantage*.
- Experience in software development using agile software development principles (as described in the scope of work and development approach section of the ToR) *would be an advantage*.
- Demonstrated experience using recommended technology stack *would be an asset*.

The Consultant 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 Client may, when necessary, visit to familiarize themselves with the systems put into operation by the Consultant) to demonstrate that it meets the qualifications requirements.

3.7.2. Consultant's Staffing

The performance of the proposed assignment will require Key Professional Staff and Non-Key Staff. The Consultant should provide qualified staff, both key-experts and non-key experts considering the assignment requirements and implementation time frame. The number and level of effort for all experts shall be listed in the technical proposal and their costs included in the financial proposal. The minimum estimated staff input is 2100 person/working days from which at least 1700 days are foreseen for the key experts. Staff inputs may be adjusted during the contract implementation, subject to actual needs and additional system functionalities to be developed.

The entire team of the proposed experts MUST jointly meet all the listed requirements:

- Proven experience in web UI design and development using responsive frameworks, progressive web apps
- Proven experience in database design, development, and optimization
- Experience in systems' integration, API design and development using SOAP/REST
- Experience with unit testing
- Experience in DevOps practices
- Experience in system analysis
- Experience as a Scrum Master in at least three projects

Qualification of Key Experts

Key experts represent specific knowledge and/or expertise required for the successful project implementation. Although the Consultant will form project implementation team at its discretion, the Consultant shall provide following key experts with proved competencies:

- Key expert 1. Project manager
- Key expert 2. Business analyst
- Key expert 3. Senior software developer / software architect
- Key expert 4. Senior software developer / software architect
- Key Expert 5. Software developer
- Key Expert 6. Software developer
- Key Expert 7. Software developer
- Key Expert 8. Software Tester
- Key Expert 9. Software Tester
- Key Expert 10. Trainer

For proposed key experts the CVs need to be submitted, demonstrating the minimum qualifications requirements, as detailed below. Reallocation of competences among key experts and/or split of key expert competences is only allowed upon receipt of prior consent of the client.

Key expert 1. *Project manager*

Project Manager will be responsible for coordination of administrative activities, such as team composition management, financial relations, reporting submission, organizational tasks for implementation stage and any other activities not covered by any other Developer Team member.

Usual set of competences of a project manager (use PMI Core Competencies Checklist[2] or similar to assess eligibility) plus:

- University degree in Computer Science or another relevant domain;
- At least 5 years of experience of IT software development and implementation projects;
- Managing of implementation of at least 3 projects of similar kind and size within 5 last years, including at least one project based on agile approach (engaging techniques like SCRUM, TDD, FDD etc.);
- Experience in IS project implementation in governmental or public sectors;
- Understanding basics of PMI / IPMA / PRINCE2 project management fundamentals, certification constitutes a strong advantage;
- Fluency in English, ability to communicate in Romanian and/or Russian languages.

Key expert 2. *Business analyst*

Usual set of competences of a business analyst plus:

- University degree in Computer Science or another relevant domain;
- At least 5 years of business analysis experience in IT / software development projects of similar kind and size;
- Fluency in English and Romanian languages;
- Deep understanding of business process management (BPM) technologies, including fluency in BPMN (ISO 19510) notation;
- Experience in implementation of BPMS systems, or IS incorporating BPM engines.
- Legal background constitutes a strong advantage;
- Understanding of enterprise lifecycle constitutes a strong advantage.

Key experts 3 and 4. *Senior software developer / software architect*

Usual set of software architect competences plus:

- University degree in Computer Science or another relevant domain;
- At least 10 years' experience in software development;
- Participation in at least 3 projects of similar kind and size in governmental or public sector during past 5 years, at least in one of them as a software architect and/or senior software developer;
- Deep understanding of modern development technologies, including web technologies and development of thin-client applications;
- Experience in development of high availability and high-performance software, as well as use of high-availability application architecture;
- At least 3 years of experience in software development using the proposed technology stack;
- Deep understanding of system integration, interoperability and containerisation;
- Understanding of business process management (BPM) technologies, including implementation of BPMS systems, or IS incorporating BPM engines;
- Participation in at least one project implemented using agile approach during past 3 years;
- Ability to communicate in English and Romanian languages.

Key Experts 5, 6 and 7. *Software developer*

- University degree in Computer Science or another relevant domain;
- At least 5 years' experience in software development;

- Participated in at least 2 software development projects in the last 3 years using agile approach;
- At least 3 years of experience in software development using proposed technology stack;
- Certifications in any technology from the proposed technology stack is an asset;
- Ability to communicate in English. Romanian will be an asset.

Key Experts 8 and 9. *Software Tester*

- University degree in Computer Science or another relevant domain;
- At least 3 years' experience in software testing in projects of similar complexity;
- Proven experience in software testing analysis and design;
- Proven experience in automated testing;
- Proven experience in performance (load and stress) testing;
- Proven experience in security testing;
- Certification in testing or any technology from the proposed technology stack is an asset;
- Ability to communicate in English. Romanian will be an asset.

Key Expert 10. *Trainer*

Trainer's participation is expected during the release stage and expected to be limited to the following three main areas: (I) User Guides drafting; (II) e-learning materials development; (III) training of the system users.

- University degree in Computer Science or another relevant domain;
- At least 5 (five) years of overall professional experience in training users in using information systems;
- Participation in at least 3 (three) projects of similar complexity;
- Significant professional experience in development of training courses and content for e-learning platforms;
- Significant professional experience in development of user guides and other training materials;
- Excellent speaking and writing in Romanian.

Although the Consultant may offer any development technology stack, programming languages and databases, that meet criteria of business and technical requirements of this document, the task of Senior software developer / software architect is to ensure the chosen technologies are in line with overall requirements for governmental systems.

Qualification of Non-key experts

During the development and implementation of the system, besides key-experts, non-key experts are required to join the team. In order to demonstrate the availability of such experts, the CVs for non-key experts should be included in the consultant's proposal.

Such CVs will not be evaluated but used to demonstrate that the Consultant has access to experts with the required profiles. The proposed non-key experts will only have to be listed in the technical proposal and indicate their costs in the financial proposal.

On Client's request, the Consultant shall be able to provide additional effort of non-key experts (e.g. IT staff for system development and implementation) to cover additional tasks during the project implementation. It must clearly indicate the experts' profile and tasks assigned so that the applicable daily fee rate in the budget breakdown is clear.

Fields of specialization required for the non-key experts are listed below:

- Software developer (at least 2 different persons);
- Database specialist;
- Technical writer;

The profiles of the non-key experts for this contract are as follows:

- Fluency in both written and spoken English;
- For Senior experts, a proven experience of not less than 5 (five) years is required in the areas relevant to their assignment;
- For Junior experts, a proven experience of not less than 2 (two) years is required in the areas relevant to their assignment;
- Proven specific professional experience in at least one relevant project to their assignment.

3.8. Timing

The tasks defined under the current assignment are estimated to be performed in 12 months – 9 months for development and 3 months of maintenance period. If new functionalities will be identified by the Client during the maintenance period, these functionalities may be implemented in additional iterations (sprints), upon availability of budget. The Consultant must provide a 12-months Warranty.

Software requirements specification (SRS)

3.9. Purpose

The purpose of the development of the Social Protection IS is to provide the National House for Social Insurance with an efficient, reliable, and modern software solution to be used as a single mechanism ensuring:

1) The record of contributors and their obligations to the state social insurance budget;

2) Nominal record of insured persons and individual record of social insurance contributions (State Register of Individual Records in the Public Social Insurance System);

3) Receipt from the State Tax Service and processing of indicators related to the declarations on the nominal register of insured persons and declarations on the calculation and use of compulsory state social insurance contributions;

4) Daily receipt from the State Treasury and processing of payments collected in the state social insurance budget;

5) Establishment of all types of pensions and social insurance benefits, as well as other social benefits according to the regulatory framework;

6) Keeping records of beneficiaries of all types of pensions and social insurance benefits and other social benefits according to the regulatory framework;

7) Recording the payment of pensions and social security benefits and other social benefits in accordance with the regulatory framework;

8) processes for obtaining operational, statistical and analytical reports on the income and expenditure of the state social security budget.

3.10. Scope

To develop IS that ensures operation of the following:

- maintaining registry of the socially insured persons;
- maintaining registry and personal accounts of contributors of all types and insured persons, processes for calculating penalties, fines, etc;
- providing rule-based automated definition of social payments and benefits;
- providing automated payment execution using MPay;
- workplaces for NHSI employees performing manual tasks;
- workplaces for technical staff of NHSI performing IS management, configuration, administration and maintenance;
- two-way integration with other systems using MConnect;
- tools enabling data upload from digitised paper-based sources and archives
- tools enabling automation of processing of reports received from SFS, payments received from state treasury to the social insurance budget;

- tools enabling generation of statistical, analytical and financial reports for each area of available data;
- tools enabling electronic document management workflows with implementation of MSign.
- Interfaces for online access of the insured persons to the available tools and data with implementation of MPower service.
- Data exchange with NHSI financial and accounting system.

The Consultant shall also ensure deep analysis of requirements and agree details with the client, prepare project related and system accompanying documentation, as well as provide trainings for staff representatives.

The Consultant shall ensure data cleansing and migration from the current existing system(s) into the new developed solution (see section 4.1.6. “Data migration”).

At the development phase the Consultant shall provide support team to assist client’s IS users and proper incident management according to “BR501: Support at the development phase” and “BR502: Development phase SLA”.

The supplier shall ensure NHSI ability to provide continuous and uninterruptible services to the public during solution development, testing, implementation and data migration.

3.11. Product perspective

The information system should be expandable by adding new functional modules, including those developed by third-party developers and/or connected as services using MConnect. Further development of the system is seen in expanding the capabilities of the automatic decision-making mechanism, reducing the number of manual operations and integration with other public and private systems connected to MConnect.

Complete digitisation of the existing paper-based registries and archives is one of the main objectives for the further development.

3.12. User interfaces

All user interfaces must be thin client interfaces. To access any IS function, including administrative functions, standard web-browser (see “TR301: UI browser requirements”) without any custom-made add-ons shall be sufficient.

Consultant has to provide trainings on the use of user interface for all key groups of users according to section 4.1.4. “Trainings”.

3.13. External interfaces

IS shall provide intersystem access using MConnect compatible interface. Interface shall be scalable to allow adding new functions and request/response message types, as well as message versioning.

3.14. Communications interfaces

All external communication interfaces are based on HTTPS protocol both for system-to-system and human-to-system purposes and shall engage appropriate security and encryption (see “TR106: Communication protocols”).

3.15. Product functions

The basic functions of the IS are:

- automate all operations related to socially insured persons, from initial registration in the system to archiving;
- automate all calculations of social payment amounts and frequencies based on rules, registry data and person related events;
- ensure two-way integration with MPay to ensure payment execution and payment status processing;
- automate all clearing and settlement operations with funding sources (state treasure accounts etc.);
- ensure reliable history of all actions and events related to socially insured persons with full guarantee of protection against any alterations, deletions, or other manipulations.
- automate all operations related to contributors starting with initial registration in the system until archiving;
- automate all operations related to personal accounts of contributors of all types and insured persons, processes for calculating penalties, fines, etc

These functions have to be implemented according to business and technical requirements, specified in sections 4.1 “Business requirements” and 4.2 “Technical requirements”.

3.16. User characteristics

User access rights shall be based on business roles in accordance to “BR106: Role-based access”.

3.17. Usability requirements

UI usability has to comply, at least, to the Jakob Nielsen's list of ten heuristics for usability.

Other specific UI usability requirements can be found in section 4. “Annexes”.

3.18. Performance requirements

IS at the time of deployment shall be designed to meet performance requirements as specified in section 4.2.2. “Performance”.

Preliminary versions, based on interim sprint deliverables, shall meet performance requirements agreed for a particular sprint.

3.19. Design constraints

IS shall be assumed as one of many e-Government system components that are being concurrently developed by many Consultants but at any given time may be at different level of readiness and accessibility.

The design of the IS should provide the possibility of working with an arbitrary number of external systems with different levels of accessibility, as well as maintaining adequate operability when any of the external systems are completely inaccessible.

From other side, IS design should ensure peaceful degradation of its own accessibility and performance, and IS should maintain adequate remaining level of functionality and accessibility should some of its parts are failed.

In conjunction with the agile implementation approach this also means, that IS shall be accessible as soon as its first functional component is ready, and then extend in functionality upon development progresses.

3.20. Standards compliance

IS should be compliant to the basic standards ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes applied mapped for Agile methodology.

All documents must be supplied in Office Open XML files (DOCX, XLSX and PPTX), ISO/IEC 29500 compliant[3].

All video material must be provided in MPEG-4 Part 14 (MP4) files, ISO/IEC 14496-14[4] compliant.

All IS data (system and user), must be kept in Unicode UTF-8 (ISO 10646) encoding.

All IS dictionaries must be based on international standards should such standards exist, and use identifiers, codes and abbreviations specified therein. This includes, but not limited to, lists of countries (ISO 3166), currencies (ISO 4217), languages (ISO 639) and so on.

All intersystem interfaces must be compatible with MConnect according to its actual version specification (latest version to be provided by EGA).

In addition, if it’s not explicitly stated otherwise, IS itself and all accompanying items (documents, file formats etc.) also must comply with all standards included in specific requirements in section 4. “Annexes”.

3.21. Verification

Verification of IS operability shall be based acceptance criteria for use cases as specified in “BR204: Technical documentation (DTS)”. Interim test scenarios shall be prepared at the beginning of each sprint, and then may be used at later stages to verify proper operability.

Verification of meeting other project requirements shall be made using check-lists.

[3] https://www.iso.org/search.html?q=29500

[4] https://www.iso.org/search.html?q=14496-14

All interim and final test scenarios and checklists must be prepared by the Consultant and passed to the client, forming a part of IS technical documentation (see “BR204: Technical documentation (DTS)”).

4. Annexes

4.1. Business requirements

4.1.1. Functional requirements

BR101: New TO BE approach

The IS shall implement and automate TO BE approach described in “NHSI TO BE” report, that is attached to this document and is interpreted as its integral part. As well as the functions and processes of the current system, that are not described in the “NHSI TO BE” report and which will be described by the consultant in the document “Detailed business processes analysis documents” (BR204: Technical documentation).

BR102: Round-the-clock operation

IS shall provide 24/7 round-the-clock operation and shall ensure all its routine technical and business operations without the need to interrupt user access and/or activities in the system.

BR103: Process-based operation

IS shall provide approach based on business rules and business processes. Those rules and processes should be configurable by users, and rule/process amendments shall not require any changes of IS program code.

There can be processes running in fully automated mode and those that require human interactions.

Processes may be initiated manually, automatically (by timer, conditions etc.) or by request via intersystem interface (from example, by request of the court, tax office etc.).

The full list of business processes (scenarios) to be configured in the IS shall be agreed with the client at the time of system implementation. Basic examples are:

- performing social payment based on person status change at the population registry (a child was born, a person died etc.);
- setting up regular social payment based on person status change at the population registry (a person is assigned disability, there was a loss of a breadwinner, woman gave birth to a child etc.);
- setting up, adjusting or cancelling regular social payment based on person age and parameters (child dependent came of age, employee reached retirement age etc.);
- adjusting regular payment amount and/or frequency based on rule change (for example, indexing of pensions);
- performing one-time payments based on rule change (like single mass social payments or previous payment adjustments).

An example of getting use case from the formalised business process along with implementation of this business process using technical architecture proposed in section 4.2.1. Architecture and technologies” are presented in “UC001: Certificate issuance in person”.

BR104: Multi-lingual interface

System interface (UI) shall be multi-lingual and initially support at least three languages: Romanian (ISO 639-1: “RO”), Russian (ISO 639-1: “RU”) and English (ISO 639-1: “EN”). Adding new languages should be possible on the configuration level, without the need of IS program code amendments.

IS shall support multi-lingual user data as well, for example ability to hold field values in Cyrillic and Latin alphabet. Based on business configuration some data fields may contain several language values simultaneously.

BR105: Use of national ID

The only allowed person’s identifier in the system is his/her IDNP. All internal links must be IDNP based.

BR106: Role-based access

All access rights in the system are based on business roles, individual access rights are not permitted. The following access right management properties shall be implemented:

- a user may belong to one or several roles, and any number of users may have the same role or a set of same roles;
- effective user rights are formed as combination of all user rights inherited from all his business roles;
- atomic right is a right on a system business or technical function, that cannot be further divided into separate subfunctions without the inevitable need to combine these subfunctions in a single business role;
- administrators are users assigned to roles, which provide access to administrative functions;
- administrators can create any number of roles and assign any number of any atomic rights to a role;
- external interfaces that let users get access to the IS must support both (a) user authentication and (b) governmental identity provider MPass;
- external intersystem interfaces shall get access to the IS based on technical user credentials associated with the interface: those should be assigned administrator-configurable roles the same way as for human users.

For human users, IS roles to apply shall be defined by their MPass roles.

BR107: Eternal record storage

Data in the system includes elements that can never be removed and should support virtually eternal storage. In particular this includes history of person social status changes and assigning/amending/cancelling social payments.

Payment history shall be kept in operational database at least two years, and then in electronic archive as required by the law (usually five years).

Record storage duration for all history elements shall be configurable by administrative users and initial values should be negotiated with the NHSI.

BR108: Task queues for performers

IS shall support queue management for all business roles and/or individual users. User shall be clearly notified that an operation requires its intervention or any activity from his/her side.

BR109: Templates

All output forms (messages, letters, documents, certificates etc.) shall be based on user configurable templates. IS shall support template versioning, and automatically switch to new template version as soon as its activation time comes. All previous versions of all templates shall remain available in archive.

BR110: Data amendments

The IS shall ensure mechanism of amendments: neither change (including mistake correction) can be made in any piece of committed data, but a new version of data element is created every time when something is being changed. At the same time mechanism of amendments adds a permanent history record, fixing the nature of change, its content, performer, and artifacts.

The correctness and validity of any element of information at any time can be checked by applying the entire sequence of all changes in their chronological order to the original version of this element of information.

In case when it doesn't compromise the performance of the IS, so called event sourcing approach may be applied, deriving actual data element state from its initial state and all subsequent amendments done.

BR111: Customer portal

Customer portal is a self-service point for NHSI clients. It is possible to get any services on the portal without personally coming to the territorial social insurance houses and contacting a specialist. The main functions of the portal are: bank accounts management where to transfer the social payments, viewing the amounts of assigned allowances, including data on seniority, requesting for any paper certificates like for submission to foreign states or for personal needs, verification of own social status, including social contributions, submission of additional information and documents signed with digital signature, sending applications for social benefits which are awarded by the request of the applicant, for example, compensation of funeral expenses and other.

Registration using MPass is required to access customer portal functions. Unlike users of NHSI workplaces that can access any data of registry of social insured persons based on privileges associated with their roles, privileges of customer portal users are limited by those associated with user IDNP.

Customer portal shall comply with all user interface requirements (see section 4.2.3. "User interface").

Design and structure of the Customer portal shall be developed by the Consultant and agreed with the client.

BR112: Reporting Tool

The System will allow back-end users defining parameters for generating reports.

The Reporting Module will enable printing reports and exporting reports using HTML, Excel, Word, xml, and pdf.

Also, the System will provide support for subscribing to the reports, by means of receiving generated reports by email in regular intervals, prepared based on defined criteria in the subscription.

UC001: Certificate issuance in person

This example case demonstrates issuance of the certificate in paper form to the single applicant. This scenario comes from TO BE version of the "NHSI Certificate issuance in person" process[5].

Use case (human actor and NHSI IS):

1. Applicant comes to the NHSI branch with its ID card.
2. NHSI specialist checks the identity of the applicant by ID card.
3. NHSI specialist using NHSI automated workplace enters IDNP of the applicant and parameters of the requested certificate.
4. NHSI specialist prints certificate created by the IS.
5. NHSI specialist signs and stamps printed paper copy of the certificate.
6. NHSI specialist passes the certificate to the applicant.

Logical steps being performed using proposed architecture (see section 4.2.1.):

1. NHSI specialist checks ID of the applicant and starts applicant's request processing using NHSI automated workplace (U14).
2. NHSI WP (U14) interacts with the validator (U01) to validate request details and place request to the command queue U02.
3. BPM engine U03 processes the request queued in U02 using the logics derived from U05, and based on respective template creates electronic form of the requested certificate. This document is placed, for a limited time, to the special section of the registry U10.
4. NHSI WP (U14) interacts with the registry U10 and gets electronic copy of the certificate from there.
5. NHSI operator prints from WP U14, signs and stamps the certificate, and then passes it to the applicant.
6. IS holds prepared certificate in electronic form for re-use within the preconfigured period of time, and then removes it to free IS resources.

The Consultant shall note that the same approach and the same tools are engaged to process online self-service requests via portal and requests placed using workplaces at the small municipalities. Further scenarios can be developed and requested by the NHSI, for example:

[5] See process No PD21030303, code STPA, ver. 1 in the TO BE report attached.

- operator may tick “Send copy by email” checkbox to instruct IS sending electronic copy of the certificate for the applicant using notification chain U06→U07→U92;
- applicant may request a certificate and get it available in his directory at the portal, thus request comes to validator U01 from the portal U15, and then it gets created certificates using chain U15→U01→U04→U10;
- applicant at the portal may request a certificate to be sent by post, so it will be created (chain U15→U01→U04→U10), printed (U10→U14), signed and then sent by post;
- etc.

4.1.2. Documentation

Documentation to be provided in unencrypted redistributable electronic form, suitable both for screen reading and printing, in Romanian language. Documents must be supplied in Office Open XML files (DOCX, XLSX and PPTX), according to section 3.20 “Standards compliance”.

BR201: User manuals

The following user documentation shall be provided:

- User manuals for users accessing the system directly (using IS workplace)
- System Functional Description
- Access Control Matrix

BR202: Administrative manuals

The following administrative documentation shall be provided:

- User administration manual
- System administration manual
- Business environment (business roles, profiles etc.) configuration manual
- Updated versions of use cases (should they change during project implementation)

BR203: Service documents

The following service documentation shall be provided:

- System installation and configuration manual
- Backup and restore manual
- Housekeeping manual
- FAQ and diagnostic (error localisation and fixing) / recovery manual
- Maintenance SLA (“BR504: Technical support SLA”)
- Risks & Issues Log

BR204: Technical documentation (DTS)

The following technical documentation shall be provided:

- Detailed business processes analysis documents that are not described in ToBe reports.

- Detailed technical documentation (DTS) – full developer's copy including architecture documentation and models
- Resource requirements for each component instance
- Pre-requisite standard software component requirements (like OS, drivers arc.)
- Professional requirements (list of required competences) for administrators and technicians who will manage and support the IS
- Test scenarios (including acceptance tests and diagnostic tests) and checklists
- Full package of documented source codes (NHSI technical staff should be able compiling these source files in fully executable system)

BR205: API and integration documentation

The following API and integration documentation shall be provided:

- API / integration manual
- samples of files and/or messages of all types
- sandbox (prototype) of API requester / responder

BR206: Video tutorials

The following video tutorials for all Actors – internal system users shall be provided:

- IS interface, login/logout, user settings
- All routine user use cases (except system administrator's tasks)

4.1.3. Legal and copyright

BR301: Software licencing

The Consultant grants to the client the rights to run and use entire solution with all included software components with no constraints and/or limitations on time, location, number of users, capacity of servers, volume of data and any others.

Should the Consultant use in its solution any licensed third-party software components and/or licensed technologies, provision of all required licences shall be arranged by the Consultant and included in project offer budget. All licences shall be produced in client's name and shall have perpetual validity (being not limited in time of use). If a licence has any volume restriction (like number of users, processors, storage space etc.), all its volume related parameters shall be sufficient for full-scale solution operations for at least three years from the time of deployment.

The client should have the right to make changes and analysis of the source code, including automated source code analysers, to detect vulnerabilities, security breaches and/or performance issues.

BR302: Business logics

The licence should clearly state that all intellectual and property rights on business logics and use cases of the system belongs exclusively to the client, including all algorithms, formulas, use cases etc.

The client preserves the right of business logic processing, amendments, duplication and/or migration to any other system.

BR303: User data

All and any piece of information except the IS source code and third party provided components form user data. It includes all pieces of information that is put into the system after its deployment by any means and in any form. User data belongs exclusively to the client.

The client preserves the right of user data processing, amendments, duplication and/or migration to any other system.

BR304: Source code

At the end of development Consultant shall supply full and actual version of all source codes of all IS components he has developed.

Should the source code include libraries or other components, that are not publicly available commercial off the shelf products, the Consultant shall provide their source codes too, as well as provide list of resources these components were taken from and indicate licences enabling to use them for the purpose of the project and further source code amendments.

For frameworks, libraries and components that are freely available, the source code shall use corresponding package managers and refer to long-term support (LTS) versions. All prerequisite software must be based on public container repositories.

4.1.4. Trainings

BR401: Training for technicians

This training is intended for client’s technician responsible for system acceptance and further inhouse maintenance. Training should include at least the following tasks related to IS:

- IS architecture
- IS technology stack
- Hardware requirements
- Third party software requirements, if any
- IS installation/reinstallation
- IS technical security and reliability features
- IS integration with other systems and/or data sources
- All technical configuration possibilities, configuration files and/or tables
- System, configuration and user data backup and restore
- All routine IS maintenance and housekeeping procedures
- IS error, fault and maloperation detection and localisation
- IS recovery procedures
- IS documentation and manuals

Consultant should inform the client in advance about prerequisite competences technicians should have prior to attend this training.

BR402: Training for administrators

This training is intended for client's administrators responsible for system business configuration, user and access rights management, daily user support and business investigations related to IS. Training should include at least the following tasks related to IS:

- IS architecture
- IS user interface
- IS security and reliability features
- Routine administrative tasks
- System configuration management
- System user and access rights management
- Audit logs
- Configuration error, fault and maloperation detection and localisation, possible user complaints and ways to resolve them
- Business configuration export/import and recovery
- IS documentation and manuals

Consultant should inform the client in advance about prerequisite competences administrators should have prior to attend this training.

BR403: Training for users

This training is intended for key client's IS users, as well as those who're responsible for providing further trainings ("train the trainers"). Training should include at least the following tasks related to IS:

- IS user interface
- Main IS features
- User environment and its configuration possibilities
- Key usage scenarios
- Documentation and where to find further information

This training should not require any IT background from attendees, basic computer usage related knowledge should be sufficient.

4.1.5. Warranty and Support

BR501: Support at the development phase

Due to agile development approach the "Working product in each iteration" principle is used. The Consultant shall provide client with technical support on functions developed during completed sprints according to "BR502: Development phase SLA", as well as provide assistance to client's IS users.

BR502: Development phase SLA

SLA between the client and Consultant at the development phase shall include reaction time (when Consultant starts working with the problem) and recovery time:

- for critical incidents (IS unavailable for the public use to retrieve information related to person's social insurance details or payment calculation/processing mechanisms fail): 30 minutes reaction time and 2 hours recovery time
- for non-critical incidents affecting the public use of the IS: 1 hour reaction time and 4 hours recovery time
- for telephone requests waiting time before a call is answered should not exceed 10 minutes during working hours (09:00 – 18:00 Chisinau time)
- for email requests response time should not exceed 2 business hours

BR503: IS warranty

IS warranty period is 12 (twelve) calendar months from the date of system acceptance by the client. During the warranty period the Consultant shall free of charge fix all defects reported by the client and solve all incidents reported by the client according to the agreed SLA (see "BR504: Technical support SLA").

BR504: Technical support SLA

SLA between the client and Consultant shall include reaction time (when Consultant starts working with the problem) and recovery time:

- for critical incidents (IS unavailable for the public use to retrieve information related to person's social insurance details or payment calculation/processing mechanisms fail): 15 minutes reaction time and 1 hour recovery time
- for non-critical incidents affecting the public use of the IS: 1 hour reaction time and 4 hours recovery time
- for other non-critical incidents: 1 hour reaction time and 2 days recovery time

4.1.6. Data migration

BR601: Completeness of data

Except otherwise agreed with the client, all data elements stored in all existing NHSI systems, including historic information, shall be migrated to the new system.

BR602: Data harmonisation

Migration shall include data harmonisation, including:

- cleansing: removing information garbage not related to anything, as well as unnecessary data element duplicates, except deliberately created duplicates for performance and other reasons;
- standardisation: transforming data elements of the same nature to the same format (for example, all dates, currencies, amounts etc.).

BR603: Transformation to events

Migration of entity related information shall be performed using amendments mechanism (see "BR110: Data amendments") in the same manner as for the new information: recording initial object state and then applying in chronological order all amendments being made.

Upon successful migration the final (actual) state of each object in the new system shall match one in the existing system(s).

BR604: Managing inconsistencies

All migration mechanisms (scripts etc.) shall perform data integrity and consistency checks before recording any piece of information in the new system. Responsible person at the client's side shall be notified should any inconsistency is discovered, and user interface of the migration mechanism shall let him/her to make a decision and restore consistency.

BR605: Iterative migration

Migration mechanisms that ensure business object data migration (in particular, entity related information) shall be designed in a manner that allows repeating execution:

- data fully migrated at previous cycles shall not be migrated again;
- data not yet migrated shall be migrated in full;
- amendments to data already migrated shall be properly applied in the new system, adding missing pieces of information;
- pieces of information with discovered inconsistencies sent for review (see "BR604: Managing inconsistencies") and skipped at this migration cycle.

BR606: Migrated data volumes

Migration mechanisms shall be designed in a manner that allows migration of large volumes of data in a sort time. In particular, volume of the active (actual) data excluding dictionaries in existing systems is estimated to be ~3TB in over than 5500 DB tables.

4.2. Technical requirements

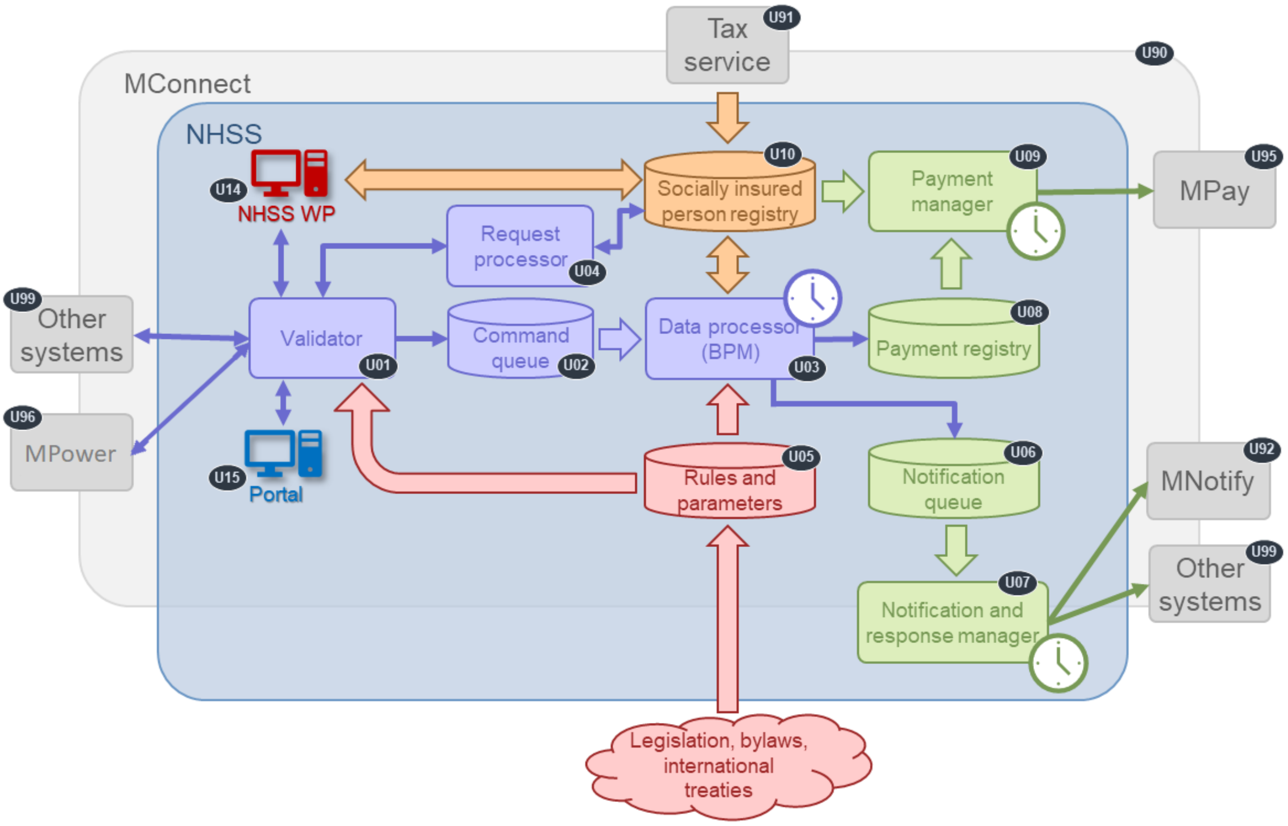
4.2.1. Architecture and technologies

TR101: Modular approach

IS solution shall be build using modular principles. Interaction of units shall allow unit replacement/upgrade without the need to redesign interacting units. SOA architecture is an advantage.

Units shall be reusable. Some units may be adopted from existing solutions already in use by the client.

Recommended high level IS architecture is presented in figure below, but will be adjusted based on the analysis and consultations with national stakeholders.



Proposed architecture includes the following units:

Unit	Name	Description
U01	Validator	Validator is the main incoming message filter. Since the IS must be integrated with various external and/or internal systems or modules developed at different time by different developers, there might come broken, unsupported and invalid messages (requests). Validator performs structural and logical message analysis and, at hight level, does one of the following: - pass synchronous command to request processor U04 and then return its response to sender; - put asynchronous command to command queue U02 and return acceptance code to sender; - return error code to sender on error.
U02	Command queue	Command queue is the place where asynchronous commands are awaiting processing by U03.
U03	Data processor (business process manager)	This is the main logical part of the system, acting in accordance with the business logics, rules and parameters kept at U05 and business data kept in various data sources, in particular: - process commands from the queue U02; - perform scheduled tasks;

Unit	Name	Description
		- perform activities should a U05 rule change; - perform activities should an insured person registry data change; - put and change payment data in the payment registry U08; - put response data and notifications to the notification queue U06.
U04	Request processor	Performs synchronous request processing and immediate data return to validator U01. It is mainly designed for real-time information request processing, while all “heavy” operations are put in command queue U02 for further sequential processing.
U05	Rules and parameters	This is the main business configuration storage. It holds both processing rules (configurable by administrators) and varying rule parameters (uploaded upon legal requirement change or by NHSI discretion). Validator U01 may use some of the rules and/or parameters performing structural and logical message checks, thus providing faster response for the requesting party and reducing load of data processors U02 and U04.
U06	Notification queue	Serves as a main outgoing message queue. May keep notifications, data requests to other IS and responses for asynchronous requests received from other IS.
U07	Notification and response manager	This unit ensures sending of messages from notification queue U06 to other systems via MConnect U90.
U08	Payment registry	The registry of all social payments to be done by the NHSI. It contains data such as the recipient IDNP, payment date and amount. The regular payments for one resident will be stored as one record with the payment period.
U09	Payment manager	Mechanism for generating payment orders. Payment manager takes information about details of payment (who and when to pay) from the payment registry U08 and the person registry U10. Payment manager sends payment information to the external system MPay U95 to make payments.
U10	Socially insured person registry	Main NHSI database (set of databases), holds all data and parameters of all insured persons and recipients of social allowances that are available in the NHSI.
U14	NHSI WP	Unified web-based (“thin client”) automated workplace for NHSI staff members. Shall automatically adapt according to configured business processes defined in U05 and particular user rights.

Unit	Name	Description
U15	Portal	Web-portal for registered users that ensures provision of all online NHSI services.
U90	MConnect	Government bus that integrates all RM government information systems (may provide services for non-government systems, too). All interactions with all external systems at U01 and U07 are performed using MConnect.
U91	Tax service	IS of the State Tax Service of the Republic of Moldova.
U92	MNotify	MNotify is a governmental electronic notification service of recipients, through various channels, regarding the events occurred upon delivery of public services or other events relevant to recipients.
U95	MPay	Mpay is RM government electronic system that allows pay for government services with any payment tool: Internet-Banking, Mobile-Banking, bank card or cash. It is used to receive payment orders from NHSI and transfer this data to banking systems or to the postal service.
U96	MPower	A reusable government service that aims to provide a secure, flexible and convenient mechanism for managing the authorization registries of individuals and legal entities.
U99	Other systems	IS of other entities that may integrate with the NHSI IS using MConnect U90 bus.

Please refer to the “NHSI TO BE” report for more details regarding current version of business processes to be ensured by the IS. Consultant shall note that those processes may change at any time and provide process management engine unit U03 flexible enough to reflect those changes (see also “BR103: Process-based operation”).

TR102: Structured history

All historic data for all past periods created in all past versions of IS should be kept in a form that allows its proper interpretation and representation regardless of current version of the IS.

TR103: Transformable data formats

All information stored in the IS shall be stored in a form allowing automated export and transformation. It preferable should be a text format, but should the storing of files (like images, scan copies etc.) is inevitable, they shall be stored only in those open standard file formats that allow unattended automated transformation to other formats without the loss of information stored therein.

IS may accept upload of files in other formats should it ensures their transformation into one of the agreed open standard file formats before saving.

TR104: Open standards

The IS architecture shall be based on relevant open standards, proprietary standards shall not be used.

TR105: Scalability, high availability and disaster recovery

The IS architecture shall support high availability, scalability and ability to work simultaneously on multiple sites and use a cloud-native architecture based on containers and container orchestration platform available in MCloud.

The IS is intended to operate in MCloud environment and has to conform with MCloud backup and disaster recovery procedures.

TR106: Communication protocols

All external communication interfaces are based on HTTPS protocol both for system-to-system and human-to-system purposes. Appropriate data protection, security and encryption shall be ensured (see section 4.2.4. “Security”).

TR107: Logs

IS shall log its activities and events in a structured form, enabling log data created in any previous IS version proper interpretation and representation in any other later version of the system. Logged fields from all IS components shall have the same format and meaning.

Event log records shall include at least the following information:

- the type of the event
- timestamp when the event took place
- event level
- system component that produced the event (event source)
- user and/or interface and/or IP that triggered the event
- information object identifier that has or may be affected
- textual details about the event

The system shall differentiate events and actions it logs into at least the following levels:

- Critical
- Error
- Warning
- Info
- Debug

Critical and Error level events shall be logged only for non-recoverable error that require human intervention. Besides logging, IS shall have administrator notification mechanism for Critical and Error level events.

System logging has to be configurable and IS shall be able to send log records to one or several log storage locations, including local and remote databases, file systems, web-services including MLog service etc.

TR108: Hardware

The IS implementation project does not include delivery of any hardware components. Upon completion IS will be deployed at the governmental cloud environment (MCloud). It is assumed that MCloud will also be used for hosting of the test system.

TR109: System operation modes

The IS shall support at least operational and maintenance modes. While operational (normal) mode enables all system functions, maintenance (restricted) mode shall prevent non-administrative users from logging in to the system, as well as disable all functions except administrative and related to IS maintenance or upgrade.

IS shall ensure graceful change of operation modes: while switching to maintenance mode IS shall stop accepting new requests, complete all started operations that cannot be queued for further execution, then notify and log off all non-administrative users, and then change its mode.

TR110: Integration

IS shall be integrated with other systems, both data providers and data consumers, using governmental MConnect gateway.

Internal NHSI systems, for performance reasons may be integrated directly avoiding MConnect, but in this case IS shall "locally" use the same (MConnect) integration protocol to allow further switch to MConnect when required.

The IS shall perform request processing the same way regardless of the interface being used: requests made via consumer portal, NHSI user workplace and received using MConnect shall be processed with the same components and according to the same logic.

TR111: Reports

IS shall incorporate report preparation engine based on user configurable templates. Preparation of all routine reports (daily, weekly, monthly etc.) and data for statistical analysis shall be automated and inattentively run in the background at the low system load time. These prepared reports and statistical data shall form a library for further consumption and/or archiving.

4.2.2. Performance

TR201: Standard load

The IS performance shall be ensured at standard load, that includes:

- 1000 concurrent human users using WP;
- 300 intersystem information requests per minute and 30 intersystem data manipulation requests per minute.

TR202: Volumes of data

The IS performance shall be ensured for 3 million active socially insured persons and 750 thousand of contributors in NHSI registry, 1,1 million data on social contributions and 1.5 million social payments per month.

TR203: Data duplication

IS has to be designed to avoid data duplication except for performance and security reasons. If duplication is considered, IS shall avoid availability of concurrent versions of the same data, retrieved from different sources.

TR204: Interoperability modes

Ensuring interoperability, IS shall support both synchronous and asynchronous request processing modes. IS shall give a favour to asynchronous (or reactive where appropriate) mode for data processing and synchronous mode for provision of information.

Where applicable user workplace shall support a sort of asynchronous mode for “heavy” operations as well, for example in a form of scenarios like “create me this report and notify when ready”, or “create this certificate and send to user by e-mail”.

TR205: User interface performance

The following interface performance criteria shall be met:

- 95% of all information requests shall be complete within 3 seconds;
- 95% of all data manipulation requests shall be complete within 5 seconds;
- 95% of all document (output form) preparation requests shall be complete within 5 seconds;
- 95% of all workplace pages shall load in 1 second if accessed using internal NHSI local area network.

The IS shall display progress indicator for all operations lasting 3 seconds or more, providing estimated remaining waiting time.

IS shall let user to interrupt any information retrieval operation and any document preparation operation that lasts more than 3 seconds.

TR206: Intersystem interface performance

The following interface performance criteria shall be met:

- 95% of all synchronous requests shall be complete within 3 seconds;
- 95% of all asynchronous change requests shall be responded within 1 second and completed (processed) if no user interaction is required within 10 seconds;
- 95% of all asynchronous data preparation requests shall be responded within 1 second and completed (processed) within 10 seconds.

4.2.3. User interface

TR301: UI browser requirements

IS workplace is a thin client: any popular web browser shall be used for accessing the system if it meets the following requirements:

- the brand of this browser is Chrome, Opera, Firefox, Edge, Safari, IE or other if its market share in Europe is at least 5%;

- the version of the browser is still supported by its developer, or the market share in Europe for this version is at least 10% among all versions of that brand.

Specific properties of operating systems shall not be used, so that any browser meeting criteria above must ensure full IS workplace functionality regardless of operating system type it works on.

TR302: Wizard-based approach

The IS where applicable should ensure wizard-based approach, that step by step leads user through operation scenario.

95% of all routine NHSI operations in the system shall be completed in no more than 10 steps (mouse clicks).

TR303: Input data validation

All input data shall be validated using against formal and logical rules both on client and server side. Appropriate messages should guide user upon mistakes.

IS should also prevent entry of any control or invisible characters, and remove them from the data elements (for example, when user use copies formatted text from external source). Nevertheless, all displayable UNICODE characters shall be preserved and must be properly displayed and/or put in output forms.

TR304: Accessibility

User interface shall conform at least to Level A of Web Content Accessibility Guidelines 2.0[6].

TR305: Responsive/Adaptive design

The system user interface shall automatically adapt to various display proportions and resolutions. Minimal display width that shall be displayed without horizontal scrolling is 1024px.

TR306: Help and hints

User Interface elements shall support hints and help elements. Texts of those hints and help elements should be adjustable by administrators.

4.2.4. Security and maintenance

TS401: Industry recognised algorithms

The IS must engage only industry standard mathematically proven algorithms and/or methods while processing, storing and communicating information.

TS402: Legislative compliance

The system shall be secure by design and comply with the relevant requirements specified in GD 201 from 28.03.2017[7] and decision of the Government of Moldova No. 1123 “Requirements for personal data protection while being processed in social security systems”.

[6] https://www.w3.org/TR/WCAG20/

[7] http://lex.justice.md/md/369772/

TS403: Least privilege principle

The IS modules and components shall rely on the least privilege principle and run under such a limited privilege account.

TS404: Secure communication channels

All IS communication with external systems or users takes place over encrypted communication channels.

User WP (browser) shall always use encrypted protocol HTTPS (RFC 2818) and refuse connection should it is not available.

TS405: Minimum web-application security

As a minimum the IS shall be secure against OWASP Top ten listed vulnerabilities[8].

TS406: User authentication

The IS should use MPass as a main user authentication mechanism for system administrators and as the only one available to other users.

IS may provide concurrent industry recognised authentication mechanisms for administrative and technical purposes (intersystem interfaces etc.).

TS407: User sessions

IS shall enable human user session management. User session should be terminated after certain configurable period of inactivity. Upon termination, user has to authenticate again and upon successful authentication should see the same screen (UI location) he saw at the moment of latest activity.

Default session expiration timeout is 30 minutes.

TS408: Unauthorised access attempts

The IS shall detect unauthorised access attempts, log them, and send configurable notifications to administrator based on failure type. The IS shall prevent unauthorised access by temporary disabling user account and/or IP address after certain unsuccessful login attempts from the same name and/or IP address (number of attempts and timeout should be configurable).

The IS should not disclose the reason of login rejection but should either display message that this attempt is recorded and there are legal consequences for unauthorised access (if direct login is used), or return generalised reject reason code (if used third party authentication, like MPass).

TS409: Data integrity

IS data integrity shall be ensured. The IS shall engage mechanisms that prevent direct data manipulation (alteration, deletion or insertion), for example by running SQL requests. All histories shall be protected using industry recognised mechanisms, for example blockchains.

Should prevention be not possible in particular situation, the IS shall make it impossible to hide the fact of manipulation and provide reliable notification mechanism for administrators.

[8] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

TR410: Automated routine maintenance tasks

All routine system maintenance and housekeeping tasks, except those that require human decisions not transferrable to logical rules, shall be automated and inattentively run in the background at the low system load time.

TR411: Monitoring and performance indicators

The IS shall expose performance and health-check metrics for third party monitoring tools (like Zabbix or Prometheus).

TR412: Start-up and shutdown

IS shall ensure graceful start-up and shutdown of its components.

When starting up, the system shall run internal integrity and security checks. System starts in maintenance mode should any significant problem is detected.

When shutting down entire system or any system component shall not affect any work in progress; first it shall stop accepting new requests, complete all started operations that cannot be queued for further execution, then notify and log off all active users, and then actually shut down.

TR413: Upgrades

System upgrades shall be automated, including database upgrade scripts or code and data transformation (migration) scripts.

Whenever possible, high-availability application architecture shall be applied ensuring seamless software upgrade without interruption of data processing and user activities. When ongoing update is impossible, the system update procedure shall only start when IS is in its maintenance mode. System can be switched back to operational mode only when upgrade procedure completes successfully or rolled back.

Consultant shall provide instructions for setting up and rolling back any system update. Updates that are irreversible (there are no feasible scripts and/or code to perform complete update roll-back and return to the previous version) shall require complete IS and its data backup before execution.

TR414: Health-check API

The system shall expose readiness and health-check API via a HTTPS GET requests. The health-check shall check the health of as many system components as possible. In case of health check error, a human-readable error message shall be returned.

TR415: IS installation

The IS and all its components has to be provided in a single package for installation by the client on the fresh and clear operating system in a form of source codes (see “BR304: Source code”).

A script to compile source codes and build production (executable) version of the IS must be provided. This script must include built-in package integrity and component version compatibility tools.