Modernization of Government Services
in the Republic of Moldova
Project ID No. P148537

TERMS OF REFERENCE
NATIONAL CONSULTANT – SOFTWARE DEVELOPER

I. 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.

From 2006 to 2013, Moldova modernized its civil service legislation and administrative processes under the Central Public Administration Reform (CPAR), supported by the World Bank's administered CPAR Multi-Donor Trust Fund.

In July 2016, the Government of Moldova approved the Public Administration Reform Strategy for 2016-2020[1], that kept the modernization of public services delivery process among its main objectives.

To achieve the stated objectives, the Government requested the World Bank's assistance for a PAR operation, that became effective in June 2018, called Modernization of Government Services Project (hereafter *MGSP* or *the Project*).

The design of the project takes into account the objectives of the Government of Moldova for inter-sectorial digitalization and makes extensive use of institutional and technological achievements of Governance e-Transformation Project (GeT) implemented by the Government of Moldova and World Bank in the period between November 2011- December 2016.

According to the National Development Plan for 2023 – 2025[2] modernization of administrative services and access of population to electronic public services are set as one if its major objectives. The Public Administration Reform Strategy 2023 – 2030[3] reconfirms the determination of the Government to modernize the administrative service delivery system by improving access to public services through various channels, their efficiency, reduction of unnecessary administrative burdens and cost of services for both beneficiaries and service providers, ensuring a stable level of quality of administrative services.

Therefore, MGSP continues to play a very important role in achieving the high level objectives set up by the Government. The project aims to improve access, efficiency and quality of delivery of selected administrative services through the following components:

1. Administrative Service Modernization

The key activities under this component focus on re-engineering a group of government to citizen and government to business administrative services; piloting of one-stop-shops for public service delivery in selected locations and rolling out at national level; increasing public awareness on and advocacy for administrative services, with a particular highlight on e-services.

2. Digital Platform and Services

The main objective of this component is to digitalize selected re-engineered government services; complete and strengthen a common infrastructure and mechanisms for rapid deployment of ICT-enabled public services; introduce government wide IT Management and Cyber Security standards and procedures. The component finances the procurement of additional shared computing infrastructure elements, digitization of services needed to deliver Government services electronically, as well as the development of a learning management system to mainstream the new digital infrastructure and the modernized services within the government.

[1] http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=366209
[2] HG89/2023 (legis.md)
[3] HG126/2023 (legis.md)

3. **Service Delivery Model Implementation**

The objective of this component is to ensure that the institutional capabilities of key government agencies are aligned with and support the new model of public services delivery.

4. **Project Management**

This component supports the Digital Platforms Unit (DPU), based in the e-Governance Agency (eGA) and ensures the activity of the core e-Governance Agency team.

Current situation in the sector

The MGSP project is designed to reuse centralized infrastructures and platforms developed by the Government of Moldova in the framework of the Governance e-Transformation Project (2010 – 2016).

One of the key areas of the e-Governance Agency activity is the implementation of the MConnect interoperability platform. Launched in 2015, MConnect interoperability platform has become the key IT Solution that ensures the automated data exchange between IT Systems.

By improving and developing an inventory of semantic assets (called Semantic Catalog), the State Chancellery and the e-Governance Agency, as coordinators of the reform of the modernization of public services, aim to provide tangible results of the reform within a short period of time.

In 2021, the Semantic Catalogue version 1.0 was deployed into production, becoming an essential tool for managing and inventorying semantic assets across public authorities. Version 1.0 provided public institutions with a structured digital repository of semantic assets, allowing for more efficient management and access to state information resources. However, while version 1.0 was a significant advancement, the increasing demands for more sophisticated data management and interoperability highlighted the need for further enhancements.

The development and implementation of version 1.1 of the Semantic Catalogue will play an important role in automating the management and inventory processes for semantic assets across public institutions in Moldova. This upgraded version introduces key enhancements aimed at streamlining workflows, optimizing user interactions, and strengthening integration with national IT platforms, particularly MConnect—the governmental interoperability platform. With the introduction of advanced filtering options, drag-and-drop functionality, bulk attribute management, and role-based access control, version 1.1 will enable public authorities to manage and configure semantic assets with greater efficiency and accuracy, significantly reducing manual interventions and potential errors.

The following entities are interested or should be involved in the design and proper functioning of the *Semantic Catalog*:

- **e-Governance Agency**, as owner of the *Semantic Catalog*, is financing the project and is an active stakeholder during the information system implementation, launch and operation, including validation and acceptance of the delivered information solution. Also, the e-Governance Agency will provide the MConnect interoperability platform for which through the Semantic Catalog will be configured the categories of data accessible to semantic assets Beneficiaries, data access strategies, and related semantic assets data.
- **Legal entities possessing semantic assets** - as proprietary of semantic assets, whose data will be provided through the MConnect interoperability platform. Semantic Assets Owners will use the Semantic Catalog for the purpose of registering and configuring semantic assets in the Semantic Catalog.
- **The Semantic Catalog** represents a key IT System for configuration and management of the inventory of semantic assets in the possession of legal entities in the Republic of Moldova. In this respect, this IT System will be the key IT resource that will provide up-to-date data on semantic assets available on the territory of the Republic of Moldova and interoperability metadata values for interaction with the MConnect interoperability platform.

- **Semantic Asset -** a data structure describing an entity, event, classifier, service, vocabulary, test data and other data elements (metadata).
- **Legal entities beneficiaries of semantic assets** - as data consumers based on semantic assets reflected in the Semantic Catalog inventory. Semantic Assets Beneficiaries will use the Semantic Catalog to explore semantic assets inventory and to request access data through MConnect.
- **IT and Cyber Security Service** (RO: Serviciul Tehnologii Informationale si Securitate Cibernetica - STISC), as MCloud owner, is responsible to provide all necessary infrastructure from MCloud to host the Semantic Catalog Information System.

II. Objectives

The e-Governance Agency seeks to recruit a National Consultant for the position of Software Developer to perform activities related to software development and support a flawless functionality of the **Semantic Catalogue Information System** managed by e-Governance Agency. The selected consultant will be responsible for executing key client-facing activities, ensuring the seamless development and deployment of the new system functionalities. Additionally, the consultant will provide ongoing maintenance and technical support.

III. Scope of Work

The scope of work for this assignment is to design, develop, configure, and deploy version 1.1 of the Semantic Catalogue Information System as a fully functional product with all new and enhanced functionalities in place. This version will address the operational challenges identified in version 1.0 and incorporate new features aimed at improving efficiency, user experience, and system integration. The development of version 1.1 will follow the specifications iteratively defined by the Client, as outlined in Annex 1, Annex 2 and Annex 3, ensuring that the final product meets the evolving needs of public institutions.
The Consultant will provide 3 months of warranty for the developed solution. The warranty period starts after final release. During the warranty period the Consultant will fix any identified defects.

The development and operations must be compliant with the legal and regulatory documents listed in **Annex 4**.

IV. Expected Deliverables

The following deliverables will be provided by the Consultant during this assignment:

1. A fully functional Semantic Catalogue version 1.1 with all the newly defined functionalities implemented and deployed in the production environment. The Consultant will deliver fully compliable, documented source code, including licenses for third-party tools and automation scripts where applicable.
2. Technical and End-user documentation developed according to the Client's documentation requirements defined in Annex 3.

Any population with or migration of data is not part of this assignment.

V. Timing

This is a short-term assignment expected to be implemented during January-April 2025.

VI. Institutional arrangements

The Consultant will work for eGA and will report to and work under the direct supervision of the appointed Semnatic Catalog Product Manager.

VII. Resources

The e-Governance Agency will provide relevant information and documents, as well as any other necessary means and support for Consultant in order to carry out this assignment. The Consultant will work remotely from his/her premises.

VIII. Skills and Qualification requirements

Mandatory qualifications:

- University degree in Computer Science or another relevant domain
- At least 7 years of 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 C#, Entity Framework, ASP.NET MVC, SQL Server and a dependency injection framework
- Certifications in any technology from the required technology stack is an asset
- Ability to communicate in Romanian or English

Annex 1. The Semantic Catalog Business Requirements

Introduction and definitions

This Annex contains an indicative set of business requirements reflecting the functionality of the *Semantic Catalog*.

1.1. Definitions

The following definitions, abbreviations and acronyms are used throughout the document unless, in the particular case, stated otherwise.

#	Acronym	Explanation
1.	**BPM**	Business Process Management
2.	**Client**	For the purpose of this ToR the client is the e-Governance Agency
3.	**Consultant**	Senior Software Developer that will design, develop and deploy the information system
4.	**DB**	Database
5.	**DTS**	Detailed technical documentation, created by Consultant, that contains detailed description of IS technical implementation
6.	**EGA**	e-Governance Agency. The e-Governance Agency will be responsible for all administrative and procedural aspects of the selection process, contract management and financial management, including payment, general project management responsibilities
7.	**GB**	Gigabyte
8.	**ICT**	Information and communications technology
9.	**IDNO**	Unique identifier of legal entity in Moldova
10.	**IDNP**	State identifier of a natural person in Moldova
11.	**IS**	Information System
12.	**LE**	Legal entity (or legal person, or juridical person) – entities such as commercial and non-commercial organisations, corporations, firms, government agencies, etc.
13.	**MB**	Megabyte

14.	**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
15.	**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
16.	**MPass**	Moldova's governmental single authentication and access control service. Ensures single sign-on and other related functionality
17.	**PAR**	Public Administration Reform
18.	**Product**	In general, includes as developed information system as results of all accompanying activities like documentation, manuals, etc.
19.	**PSA**	Public Services Agency of the Republic of Moldova
20.	**RM**	Republic of Moldova
21.	**SRLE**	Information System State Register of Legal Entities under the Public Services Agency of the Republic of Moldova
22.	**UI**	User interface, a part of IS intended for interaction between the human user and the system
23.	**US**	User story is a work item type used in agile project management to define a single piece of desired functionality from the end-user perspective. It typically includes a brief description of the feature, acceptance criteria, and any necessary details or attachments to guide development
24.	**WB**	World Bank
25.	**WP**	IS user workplace
26.	**Work Package**	The work package(s) defines the releases and iterations (Sprints in Scrum) that are contained in that stage. The content of work packages will be broken down or transformed into lower-level plans, such as release plans and iteration plans, which may be in the form of backlogs

Semantic Catalog – the information system representing an inventory of semantic assets, including management of their lifecycle[4].

[4] Law 142/2018, art.10, art.3

Semantic Asset – an identifiable set of reference data (code lists, taxonomies, dictionaries etc.) and data describing other data (metadata) used for data exchange to ensure the same meaning of the data (semantic interoperability)[5].

Conceptual semantic asset structure:

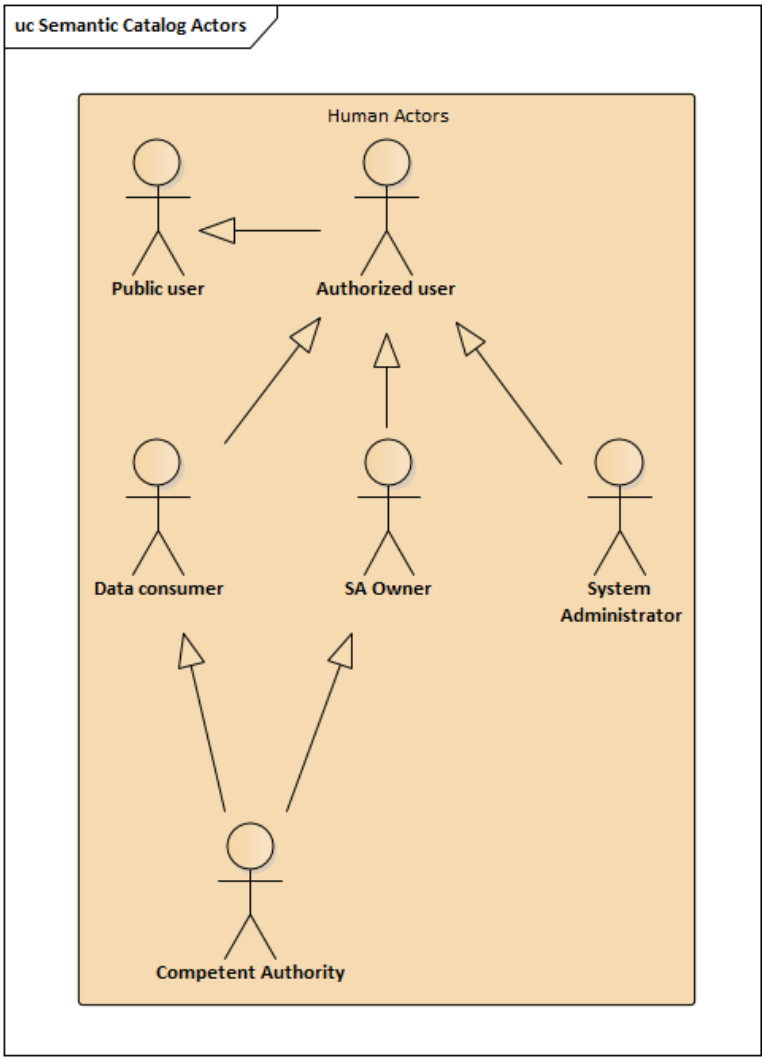
- asset identifier;
- asset name;
- asset owner;
- references to legal basis for the asset;
- asset categories;
- asset description;
- asset version number;
- asset status (draft, submitted, approved-active, approved-obsolete, rejected);
- asset type from a predefined list of types (entity, event, classifier, service, vocabulary, test data, etc.);
- asset attributes, including attribute type (primitive type or reference to another semantic asset or inline type definition), validation rules for each attribute, attribute multiplicity, attribute description;
- validation rules;
- relationship and references to another assets (like parent type, derived types);
- specific values (for classifiers, etc.)
- sample data (sample valid instances, requests, responses, etc.);
- version history;

Data exchange request – an official request for accessing data defined in semantic catalog, through interoperability platform MConnect[6].

Semantic Catalog Actors

[5] Law 142/2018, art. 3
[6] Law 142/2018, art.6, art.7

The Actors of the *Semantic Catalog* are described in the figure below:



- **Public user –** a human actor representing an anonymous public user. This user can explore the Semantic Catalog public interface (search for semantic assets, view and download details of the semantic assets, access public reports and performance indicators etc.);
- **Authorized user –** a human actor representing an authenticated user based on its electronic identity, who is authorized to use the Semantic Catalog non-public functionalities.
- **Data consumer** – a human actor representing an organization requesting access data through MConnect, based on semantic assets.
- **Semantic Assets Owner** – Representative of an organization owning semantic assets.
- **Competent Authority** – Representative of the *Competent Authority as per law 142/2018* which is in charge of management the *Semantic Catalog,* reviewing and approving data access requests.
- **System Administrator** – A user who is in charge of technical administration of *Semantic Catalog.*

User Stories linked to functional Use Cases (available in Annex 2)

US01: Advanced search capabilities for Authenticated Users

As an authenticated user (Administrator, Manager) I want to explore the catalog using advanced search options (filter by asset owner) so I can find relevant semantic assets more efficiently.

Acceptance criteria:
The Authenticated user can use filters to narrow down searches.

Linked to existing use case:

- *UC01 - Explore public content of the Semantic Catalog* but related for Authenticated user.

US02: Bulk management and drag-and-drop for semantic assets

- As an authenticated user (Administrator, Manager, Semantic Assets Owner - Operator, Data consumer[7]), I want to be able to manage assets in bulk (add, modify, delete) and utilize drag-and-drop functionality to move assets between parent and child structures, making it easier to organize and update large volumes of data
- Drag-and-drop functionality from parent to child semantic asset and vice versa for easier structure and attribute management
- Option for asset owners to perform bulk deletions across multiple assets or asset attributes at once

Acceptance criteria:

- Users can select multiple assets or attributes to add, modify, or delete in bulk within a single action.
- The system provides a confirmation prompt for bulk operations (e.g., deletion) to verify intent.
- Bulk addition and modification operations apply the same validation checks as single-item operations.
- Users can drag and drop assets between parent and child structures or move them within hierarchical structures to simplify asset organization.
- Any structural changes (e.g., moving assets) reflect immediately within the system's catalog structure, with updates visible to authorized users.
- Deletion requests for active assets are submitted for approval (if required) and processed once authorized.
- The catalog view and relevant asset metadata are updated to reflect any bulk actions taken.

Linked to existing use case

- *UC05 - Add semantic asset*
  Extension: Adds bulk addition functionality to streamline the process for high-volume updates.
- *UC06 - Modify semantic asset*
  Extension: Adds bulk modification capabilities and drag-and-drop functionality to facilitate easy asset structuring.
- *UC07 - Delete semantic asset*
  Extension: Enhances deletion options to allow bulk deletion for multiple assets or attributes in a single action.

US03: Modify and version semantic assets with semantic links

[7] For Data consumers (users requesting access to specific data assets), multiple assets or attributes can be selected for deletion in a single action. This deletion option is only available within the context of a data exchange request

As an authenticated user (Administrator, Manager, Semantic Assets Owner – Operator) I want to modify existing assets in Published state, while maintaining semantic meaning links, so I can ensure data consistency and version control across updates.

Acceptance criteria

- Modifications preserve existing semantic meaning links, ensuring that attribute updates do not disrupt established relationships.
- The system updates asset metadata and status, accordingly, ensuring only approved versions are visible to public users.

Linked to existing use case

- *UC06 – Modify semantic asset*

US04: Data exchange request with signatory approval

As an authorized user (Data Consumer), I want to submit data access requests that require approval from designated signatories before submission. The system should validate that I belong to a registered legal entity (as an employee, employer, or administrator) to ensure that I am authorized to sign and circulate the request within the entity. This validation should support both entities with an IDNO and those without, providing flexibility for diverse entity structures (e.g. IDNP, or other valid identifiers for notaries or lawyers, etc.).

Acceptance criteria:

- Draft saving: users can save draft requests to be reviewed and approved by designated signatories within their entity.
- Notifications: users receive notifications on request status changes (e.g., Received, Processing, Approved, Rejected).
- Entity validation: the system validates the authenticated user's affiliation with a legal entity (as employee, employer, or administrator) before allowing them to sign or submit a request.
    - A web service provided via MConnect validates user affiliation using:
        - RSUD for administrator verification
        - CNAS service to confirm employment with the entity
- Request visibility:
    - The request is visible only to the user who created it and to the administrator/manager of the legal entity, ensuring controlled circulation within the organization.

Linked to existing use case

- *UC12 – Submit request for data access.*
  Extension: Ensures only validated users within a legal entity (or service providers with valid identifiers) can submit, circulate, and sign requests, adding entity-based control to the request submission process.

US05: AGE Request Manager role for managing MConnect connection requests

As an authenticated user with the role of Request Manager, I need to manage MConnect connection requests within the Semantic Catalog, including visualizing all requests, updating request statuses, and accessing an organized view with countdown timers to ensure timely processing. When I change the status of a request, the Data Consumer who submitted it should automatically receive a notification about this update, enabling transparent and timely communication.

Acceptance criteria

- Request visualization
    - Request Managers can access a dedicated view showing all MConnect connection requests in the Semantic Catalog.
    - Requests are organized by status: Waiting for processing, in Review, Submitted for adjustment, Processed positive and Processed negative
- Status management
    - Request Managers can update the status of each request to:
        - Waiting for processing
        - In Review
        - Processed positive
        - Processed negative
        - Forwarded for adjustment
    - Status changes are saved in real-time, with details updated to reflect the latest action taken.
- Automatic notification upon Status change:
    - When the Request Manager changes the status of a request, the Data Consumer who submitted it automatically receives a notification informing them of the new status.
    - Notifications are accessible to the Data Consumer in the Notifications section and on Data exchange request page within the Semantic Catalog, allowing them to track request progress and stay updated.
- Sidebar and menu organization:
    - A dedicated MConnect connection requests section is added to the Sidebar menu, allowing Request Managers to quickly navigate to:
        - Requests waiting for Processing
        - Requests in Review
        - Requests submitted for Adjustment
        - Processed Positive requests
        - Processed Negative requests
    - Requests in Review subcategory includes a countdown timer for processing timelines.
- Countdown timer:
    - Each status update triggers a 30-day countdown timer, ensuring Request Managers are aware of processing deadlines.
    - The countdown clock is only reset when the request status is changed to "Submitted for Completion/Modification/Adjustment," allowing additional time for required adjustments.

Linked to existing use case

- *UC12: Submit request for data access:* this use case allows Request Managers to view, update, and manage MConnect connection requests efficiently, with automatic notifications and organized request management tools.

UC6: Generate Reports and Statistics

As a user (any role), I want to access summary reports within the Semantic Catalog that provide insights into data exchange requests, asset additions, and usage over specified periods (e.g., 3 months, 6 months). This will help me understand overall activity trends without requiring access to sensitive or detailed data.

Acceptance criteria

- Report access:
  - Users can access the following summary reports:
    - Asset addition summary: displays the total number of new assets added within a selected timeframe.
    - Asset usage overview: shows general statistics on asset usage and access counts, without disclosing sensitive or detailed modification histories.
    - MConnect request summary: provides an overview of the number of MConnect connection requests processed, categorized by basic statuses (e.g., Submitted, Processed).
- Date range selection:
  - Users can select from predefined date ranges (e.g., last 3 months, last 6 months) to view trends over different timeframes.
  - Reports reflect aggregated data from the selected date range, ensuring privacy and maintaining public access limitations.
- Report format:
  - Reports are available in the Semantic Catalog interface, with options to download a simplified .XLXS summary.
- Privacy and data sensitivity:
  - Reports provided to users do not include sensitive details (e.g., asset owner information or detailed request content) and are limited to aggregated statistics to ensure compliance with privacy requirements.

Linked to existing use case

- *UC13: Generate reports and statistics*

UC7: Upload classifiers using Excel with automatic validation

- As an authenticated user (Semantic Asset Owner, Administrator, or Asset Manager), I want to upload classifiers through Excel files so that they are automatically validated and displayed on the platform in accordance with the system's structure. This will enable efficient and accurate classifier management for users with access permissions.

Acceptance criteria

- File upload:

    - Semantic Asset Owners, Admins, and Managers can upload Excel files containing classifier data directly through the platform's interface.
    - The system accepts files in Excel format (.xls, .xlsx) and provides feedback if the format is incorrect.
- Automatic validation:
    - Upon upload, the system automatically validates the classifier data to ensure it conforms to required structures and formats.
- Validation checks include:
    - Correct data types and field formats.
    - Required fields are populated.
    - Data integrity checks (e.g., no duplicate entries or invalid characters).
    - Users receive immediate feedback on validation results, highlighting any errors or issues in the uploaded file.
- Display and integration:
    - Once validated, the classifier data is displayed on the platform in alignment with the system's structural requirements.
    - The data integrates seamlessly into existing classifiers, making it accessible for system functions and user interactions.
- Error handling:
    - If validation fails, users receive a detailed error report listing issues for each row or column, allowing them to correct and re-upload the file.
    - The system retains no partial data if validation fails, ensuring only fully valid data is displayed.

Linked to existing use case

- *UC05: Add semantic asset*

Annex 2. Business functions of the Semantic Catalog version 1.0

UC01: Explore public content of the Semantic Catalog
Public user can explore content of the *Semantic Catalog* by:

- searching semantic assets;
- listing categories;
- listing semantic asset owners;
- viewing semantic asset details;
- downloading technical specifications for a semantic asset (CSV, XSD, JSON schema, WSDL, etc.);
- referencing semantic asset by using user friendly URL;
- view statistics about semantic assets.

UC02: Login
Public user can login into *Semantic Catalog* using MPass[8] in order to access additional functionalities if authorized.

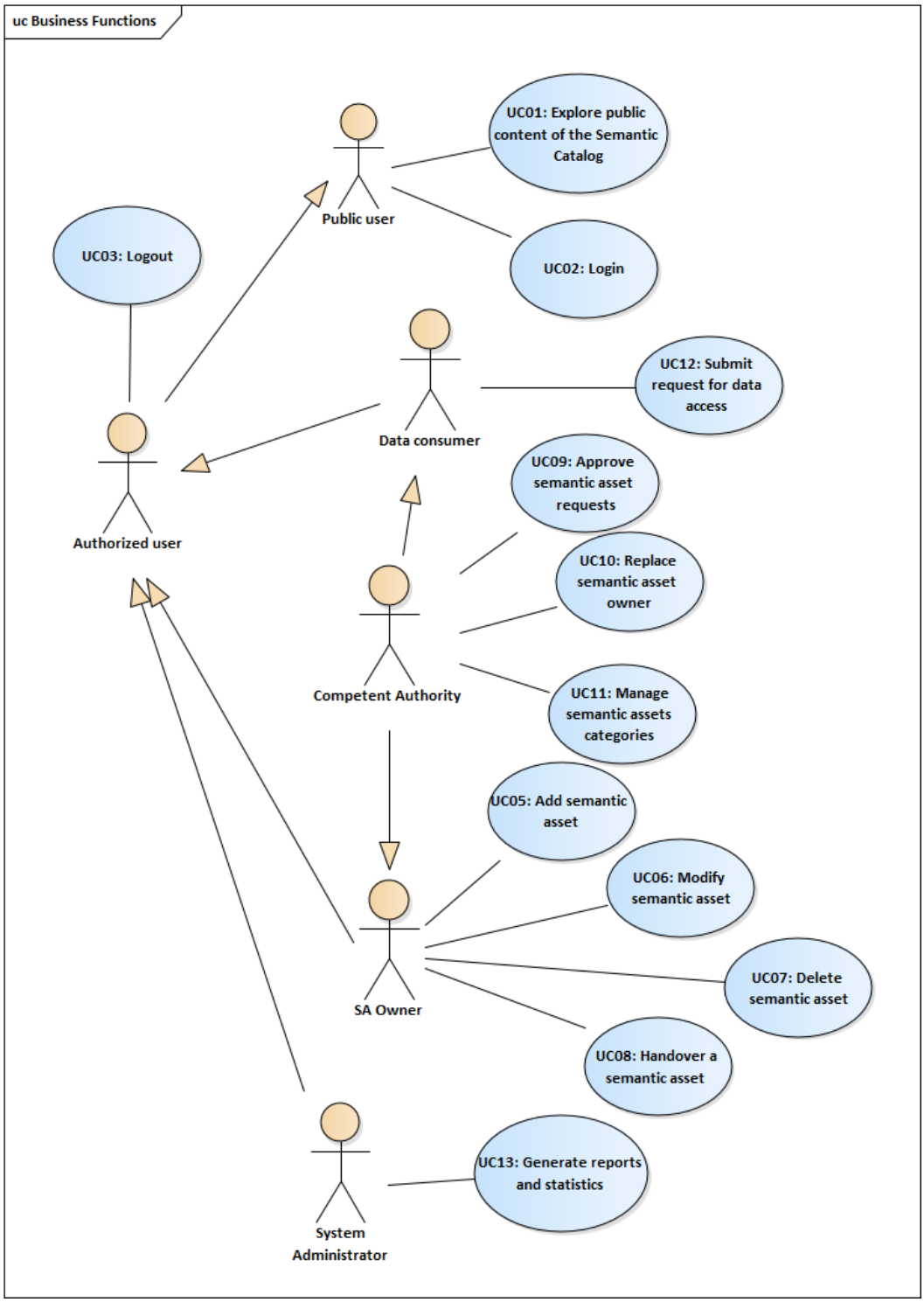
UC03: Logout
An authorized user can sign-out of *Semantic Catalog* thus closing a working session.

UC04: *User management (out of scope)*
Before defining new semantic assets, an organisation (owning semantic assets) must designate a person as a representative of the semantic asset owner to manage its assets.

Competent Authority representative and the *Semantic Catalog* administrator is designated by EGA in the same manner.

These designations happen outside of the *Semantic Catalog* and the authorisation information is provided by MPass as one of authentication attribute.

[8] https://mpass.gov.md



UC05: Add semantic asset

Semantic asset owner can add new semantic assets by defining and submitting them for approval.

Semantic asset definition includes at least the following:

- specifying the asset type from a predefined list of types (entity, event, classifier, service, vocabulary, test data, etc.);
- setting all required properties;
- validating asset consistency;
- generating asset identifier;
- saving to drafts (optional);
- submission to *Competent Authority* for approval.

UC06: Modify semantic asset
Semantic asset owner can select an existing and active or draft semantic asset and modify. Each modification of an approved asset implies creating a new version of it. The modifications are performed like initial asset definition.
The new version uses the same identifier and an incremental version number.

UC07: Delete semantic asset
Semantic asset owner can request deletion of an active asset.

UC08: Handover a semantic asset
The semantic asset owner can request the reassignment of the ownership to another organization by specifying the legal reasons and suggesting the new owner.

UC09: Approve semantic asset requests
The Competent Authority approves the semantic asset registration, modification, reassignment and deletion requests. The changes semantic assets are effective upon approval.
In case of inconsistences in semantic asset definition the Competent Authority will reject the request with appropriate documented reason.

UC10: Replace semantic asset owner
The Competent Authority can replace the asset owner. The reasons for owner replacement may be explicit request from current asset owner, ordinary asset assignment, reassignment as result of institutional reforms or as a result of inconsistent registration (duplication, collision, overlap, etc).

UC11: Manage semantic assets categories
The Competent Authority can manage semantic asset categories by creating, modifying, deleting categories and subcategories. The categories are used by the semantic asset owners for organising semantic assets.

UC12: Submit request for data access
The authorized user can fill in, upload or reference relevant documents, sign the request for data access through MConnect platform and submit it to Competent Authority for processing. The request shall reference existing semantic assets from the Semantic Catalog or request specific semantic assets (new, modified or combined semantic assets).
The request for data access will be processed by the Competent Authority in an external system which will receive the requests through an API which will be defined during the implementation phase.

UC13: Generate reports and statistics
The Competent Authority, semantic asset owner and system administrator can generate pre-defined administrative reports based on events of the Semantic Catalog.
The type of the reports will be defined during the implementation.

Annex 3. The Semantic Catalog Technical Requirements

Documentation requirements

User Documentation	The Consultant will prepare and deliver the following documentation for end-users: • Downloadable user manual in PDF format for Semantic Catalog, Administrator, etc. All end-user documentation will be provided in Romanian.
Technical documentation	The Consultant will prepare and deliver the following technical documentation: • System architecture documentation (including description of models in UML language, which will include a sufficient level of details of the system architecture) • Test strategy • Compilable and documented source code for applications, components and unit tests developed within the project • System installation and configuration manual (including code compilation, container image build scripts, system installation, hardware and software requirements, platform description and configuration, backup and disaster recovery procedures). All technical documentation will be provided in English.
API documentation	The Consultant will prepare and deliver: • API integration guide • Integration samples in .NET and Java • Human and machine-readable description in a standard description language (e.g. WSDL or Swagger). All API documentation will be provided in English.

Rights requirements

Perpetual software license	The Consultant grants to the Client the rights to run and use entire solution with all included software components with no constraints on time, location and offered functionality.
Redistribution rights	The Consultant shall grant to the Client the right to re-distribute the solution. While the Client does not intend to re-distribute at a massive scale it still envisions the need to transfer the software solution to another state agency due for example to potential reorganization. Also, the Client might get the opportunity to re-deploy the entire e-Government platform (Semantic Catalog) elsewhere.
Full data rights	The Client keeps full rights on data created by the means of this solution.
Open data format	The solution stores the data in an open format or includes mechanisms to extract data from the system in an open format thus enabling the capability to transfer/migrate the data to another system.

Architecture requirements

Open standards	The solution architecture shall be based on relevant open standards. The solution architecture shall not use proprietary standards.
Service Oriented Architecture	The solution shall be based on a Service Oriented Architecture.
Hosting environment	The solution shall not include any hardware components and upon finalization will be deployed on governmental cloud environment (MCloud).
Running environment	System shall run on Docker container engine and shall not depend on specific host OS instance. Building container images shall be automated. (refer to the following link for details: https://docs.docker.com/develop) Running in a container-based environment, the application must be elastic, including when adding/removing application container instances (above minimum required instances for HA), changing of configurations and system parameters has no impact on any work in progress, such as any active sessions, requests, etc.
Multiple sites	The solution architecture shall ensure high availability including during new versions deployment and the possibility to run simultaneously on multiple sites
Browser compatibility requirements	The system shall be compatible with latest two major versions (to be considered at the time of system acceptance) of following web browsers: Chrome, Safari, FireFox and Edge.
API for integration with governmental platform services and third-party systems	The Semantic Catalog Information System shall expose API for functionalities to be consumed by governmental platform services (at least for MPass, MSign, MLog, MNotify) and by third party systems. The full list of logically applicable APIs and their format will be detailed during analysis and design stages.
Detailed data model	System's detailed data model shall be described fully in a machine-readable data scheme for example using a DDL language for relational databases. The Consultant shall coordinate the detailed data model schema format with the Purchaser in advance.

System Performance requirements

Asynchronous processing	System shall use asynchronous processing whenever possible to perform any input-output.
Concurrent users	The system must be capable to allow simultaneous activity of minimum 50 users at level of *Beneficiary of Semantic Assets, Owner of Semantic Assets, Competent Authority, System Administrator* and over 100 users at level of *Public User*.

Concurrent system requests	The system shall be designed to respond (via API requests) to at least 200 concurrent external system requests.
Response time	Response time for system functions shall be under 3 (three) second. The Consultant shall list the exceptions, if any, and discuss/agree them with the Client at analysis and design stages.
Daily transactions	The system must be capable to allow activity of over 1000 authorized users of category *Beneficiary of Semantic Assets, Owner of Semantic Assets, Competent Authority, System Administrator.*
Yearly transactions	• The system must be capable to allow yearly activity of over 10000 users of category *Public User.* • The system must be capable to annually process and store over 1000 electronic forms of requests for authorization of legal entities to *Semantic Catalog,* semantic actives registration/update, and access to data of semantic actives.
Key performance Indicators	The system shall meter and expose its key performance indicators. The Consultant shall propose the list of indicators and discuss/agree them with the Client.

User Interface requirements

User Interface accessibility	User interface shall conform at least to Level A of Web Content Accessibility Guidelines 2.0. https://www.w3.org/TR/WCAG20/
Responsive/Adaptive design	The system user interface shall automatically adapt to various display resolutions. Minimal display width is 480px. The system's UI shall be implemented using progressive web application (PWA) technologies and shall be functional on mobile devices.
Contextual help	User Interface elements shall include Tips and Hints for user interface elements.
Client support	All pages shall include client support contacts.

System maintenance requirements

System logs	The system shall log its various actions and events in a structured manner. Logging shall be configurable and based on extensible logging framework (such as log4net, nlog, etc.). Logging framework shall minimally support JSON format and the following targets: console, rolling files, UDP and HTTP POST.
Log levels and event log records	• The system shall differentiate events and actions it logs into at least following levels: Critical, Error, Warning, Info, Debug • Critical and Error level events shall be logged only for non-recoverable error that require human intervention.

	• Event log records will include at least: • the type of the event • timestamp when the event took place • event level • system component that produced the event • user/user agent, IP that triggered the event • information object identifier affected textual details about the produced event
Graceful shutdown	The system shall implement graceful shutdown, i.e. shutting down an application container instance at any time shall not impact any work in progress, such as any active sessions, requests, event logs, etc.
Source code	The Consultant shall supply all the source code for system components that are not available as COTS from third parties. The source code shall use package managers for dependencies to 3rd party libraries. All prerequisite software must be part of container image definition and based on public container repository.
System deployment	The Consultant shall supply the deployment procedure and supporting tools for this. Deployment procedure shall cover all the prerequisites before proceeding to system installation. The deployment shall be automated and include database structure initialization and seeding.
System upgrades	System upgrades shall be automated, including database upgrade/downgrade scripts or code. To enable rolling upgrades in production environment, the recommended practice is to perform database breaking changes in incremental changes.

Security requirements

Secure architecture	The system shall be secure by design and comply with the relevant requirements specified in GD 201 from 28.03.2017 (http://lex.justice.md/md/369772/). The Consultant shall supply documentation describing this design and supporting evidences that such a design is secure. Note that the Consultant will coordinate with the Purchaser the format of the documentation, supporting evidence and list of requirements to comply with.
Least privilege principle enforcement	The system's components shall rely on the least privilege principle and run under such a limited privilege account under the OS rights model. The documentation shall highlight each of the system's components required privilege level and considerations that force use of that level or access.
Secrets and addresses	Secrets (passwords, private keys and certificates, connection strings) and addresses of external services shall be clearly delineated in configuration documentation and easily modifiable via automated scripts.
Secure communication channels	All system's communication with external systems or users takes place over encrypted communication channels.

No Username/Password authentication	The system shall rely on authentication via MPass. Other forms of user authentication shall not be used.
Minimize personal information storage	The system shall minimize the amount of personally identifiable information stored. For example, there is no need to store a user's First and Second names since this will be provided after authentication by MPass. The system shall comply with the relevant requirements related to personal data processing specified in GD 1123 from 14.12.2010 (http://lex.justice.md/md/337094/) Note that the Consultant shall coordinate with the Purchaser the list of requirements to comply with.
Secure against OWASP Top 10 vulnerabilities	The system shall include security controls for all its components for at least OWASP Top 10 vulnerabilities. Refer https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
Health-check API	The system shall expose readiness and health-check API via a HTTP 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.
Session expiration	The system shall include a session expiration mechanism when after a specific period of inactivity, the user is required to authenticate again. The period of inactivity shall be configurable and by default it is 15 mins.
Input validation	All input data shall be validated on client and server side.
User content	User content can be captured in text format only. The system shall forbid entry of special characters used for formatting and markup of special Web content. Otherwise all UNICODE characters shall be possible to enter/view by system's components.
Unauthorized access attempts	Unauthorized access attempts When the system registers unauthorized access attempts it shall: • log such attempts with at least ERROR level • provide users with a warning message that access is not authorized and that abuse will be investigated
Data integrity	The Consultant will ensure data integrity by providing appropriate solution for prevention of unauthorized internal activities (for ex. deletion of authorizations records directly from database).

Support and Warranty requirements

Support	During the warranty period the Consultant shall provide necessary technical assistance to the Client;
Warranty	During the warranty period the Consultant shall: • fix all defects reported by the Client;

	• solve all incidents reported by the Client according to the agreed SLAs; Note: The response and resolution time shall not exceed 60 minutes for non-critical errors and 15 minutes in case of critical errors. The incidents shall be solved within 2 working days for non-critical errors and within 4 working hours for critical errors starting from escalation time. Hourly progress report will be provided for critical errors.