Terms of Reference

Consulting services for the design, development, configuration, and deployment of the MobiSign information system prototype

1. Background

The Government of Moldova is determined to fundamentally change the way 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 is the modernization of public services.

A large part of public services in Moldova are offered electronically, require strong authentication and documents with digital signatures. Governmental service for electronic signature MSign is being widely used by electronic systems for signature of the digital documents using the available digital signatures: mobile signature offered by GSM providers; electronic signature using hardware tokens provided by the governmental Service for Informational Technology and Cyber Security; and Electronic ID card issued by the Agency for Public Services. During the several years of use of these electronic signatures we observed that technologies used have some issues that restrict some potential users to become digital signees.

To solve the big part of the existing issues and increase the security of digital signing process Agency for Electronic Government developed a new concept of electronic signature, that will not depend on hardware or private provider.
Modern cryptographic research, the ubiquity of mobile phones, and international practice has shown that there are equally secure alternatives for keeping your private key private that do not require specialized physical devices. A viable, affordable, and secure alternative solution is to split the private key into two components and keep them with both participants in the process: one part in the mobile phone under the exclusive control of the holder and a second part with the e-signature service provider. This ensures that the private key cannot be compromised by compromising the mobile device alone, but also guarantees full control of the holder over the e-signature creation process. In other words, the signature can only be created with the participation of both parties in the process, with the holder having control over the process, while the provider can ensure its security, including by blocking the use of the private key when the PIN is entered incorrectly and repeatedly.

2. Objective of the Assignment

The Client is looking for an ICT consulting company to develop the MobiSign Information System Prototype with demonstrated experience in the design and implementation of complex mobile applications.

3. Scope of work and Development approach

The scope of work of this assignment is to design, develop, configure the information system as a prototype product with basic functionalities in place, according to the specifications iteratively identified and defined by the Client (the indicative set of requirements is listed in Annex 1 and Annex 2) 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.

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.

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.

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 criteria – Definition of Ready (e.g. 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, including possible visits to Client site. Working products from different sprints can be combined into a release deployed in production at Client's discretion.

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 – is 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; s/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.

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 owner will maintain the product backlog up to date, so it reflects prioritized list of desired functionalities.
- Answering to questions coming from developers – the 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 to track progress and to ensure the appropriate product development.

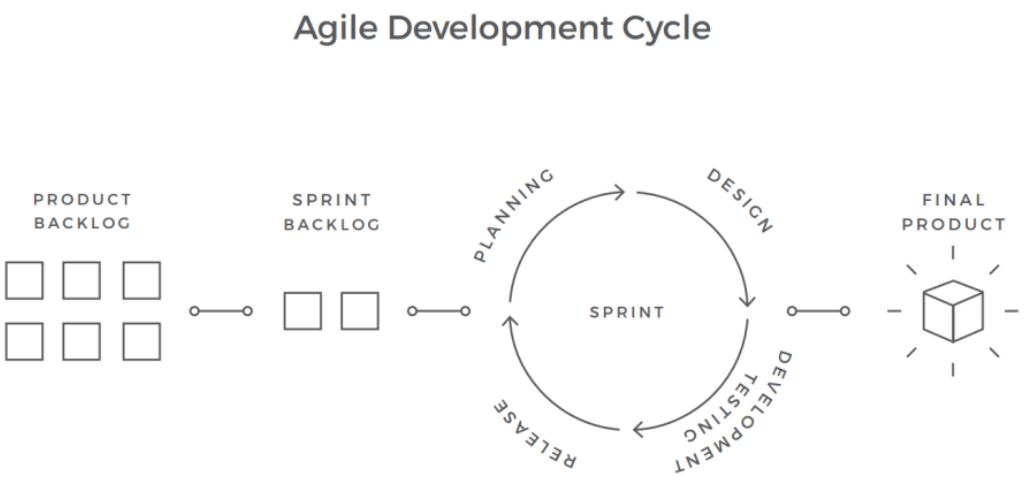

Figure 1. The indicative illustration of the Agile Development Cycle/Process

Required technology stack
To preserve e-Government investments, as well as to take advantage of cloud-native and mobile-native features, the solution shall be developed using the latest versions of the following technology stack:

- For Backend/BackOffice:
  - Programming language is C#.
  - ORM is Entity Framework Core.
  - Web framework is ASP.NET MVC Core.
  - UI framework is Bootstrap.
  - UI component framework is Blazor.
  - Package manager for components is NuGet.
  - RDBMS is SQL Server.
  - Container orchestrator is Kubernetes.
- For Android development:
  - Programming language is Kotlin.
  - UI framework is JetPack Compose.

- For iOS development:
    - Programming language is Swift.
    - UI framework is SwiftUI.

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 these shall be added through amendments to the contract.

4. Expected Deliverables

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

- A prototype of the MobiSign information system with both native mobile apps, for Android and iOS, and functionalities developed and deployed according to the requirements defined by the Client during the assignment. The Consultant will deliver compliable and documented source code (including third-party tools and libraries, licenses, where applicable and automation scripts).
- Documented integration points for Governmental Authentication and Authorization Service (MPass).

5. Reporting Requirements

The following reports will be provided during the assignment:

- Finished Sprint Report, for each completed sprint, including release notes, breakdown and duration of tasks implemented during the sprint, velocity, issues and outstanding problems, proposed actions to be taken;
- Next Sprint Backlog, including breakdown and estimated duration of tasks proposed to be implemented during the next sprint, resources that the Consultant expects to be provided by the Client and/or actions to be taken by the Client.

6. Timing

The tasks defined under the current contract are estimated to be performed in 3 months for development and delivery.
Subject to satisfactory performance and budget availability, the contract can be extended based on the same fee rates.

7. Institutional arrangements

The Client is responsible for all administrative and procedural aspects, contract and financial management, including acceptance and payment of deliverables/reports expected under the Contract, general project responsibilities and efficient coordination with stakeholders.

A Product Owner will be appointed by the Client and will coordinate and decide on all issues related to the technical elements of the Contract. The Product Owner will issue the administrative notice on the start date of the implementation of the contract and other administrative duties.

The Client will provide the following:

- infrastructure resources for testing environments;
- code repository, issue tracking system, CI/CD environment, task management system via the Client's subscription in Azure DevOps. The Consultant shall not include Azure DevOps subscription in its financial proposal;
- access to Client's Google Play and Apple Store accounts, as necessary.

The Consultant will ensure that adequate working conditions (workspace/office premises for experts, office equipment, computers, communication facilities, etc.) and services are provided to the Consultant's staff during the lifetime of the project.

The Consultant will be responsible for the day-to-day management of the project team and availability of necessary resources.

The Consultant will organize the Kick-off meeting and initial Backlog discussion at its premises or online. All Consultant's Key Experts as specified in the section defining the qualification requirements, shall participate in person or remotely in the kick-off, planning and review meetings.

In case the deliverables contain defects and/or there are delays for reasons not imputable to the Client that may impact project outcome, the Consultant may be requested to visit the Client's site in order to solve the project issues.
The communication languages will be Romanian or English.
The Consultant shall work under the supervision of the appointed Product Owner and report to the Client's Project Manager.

8. Qualification Requirements

Consultant qualifications 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 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 following experience requirements:

- Have been in operation for at least five (5) years with main part of its business being the development of information systems.
- Experience in development of at least (2) solutions that involve native mobile applications finalized in the last (5) years.
- 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 asset.
- Demonstrated experience using required technology stack would be an asset.

Staff qualifications requirements

The Consultant shall provide a team of the following key experts:

- Key expert 1. Backend senior software developer
- Key expert 2. Backend/Frontend software developer
- Key expert 3. Android senior software developer
- Key expert 4. Android software developer
- Key expert 5. iOS senior software developer
- Key expert 6. iOS software developer

Each key expert must meet at least one the following requirements:

- Proven experience in web UI design and development using responsive frameworks
- Proven experience in database design, development, and optimization
- Experience in systems' integration, API design and development using SOAP/REST
- Experience with native Android mobile development

- Experience with native iOS mobile development
- Experience with unit testing
- Experience in DevOps practices
- Experience in system analysis.

Per total the entire team of the proposed key experts must meet all the above requirements. Offers which will not demonstrate that the team covers the above requirements may be subject of disqualification.

For proposed key experts the CVs need to be submitted, demonstrating the minimum qualifications requirements, as detailed below:

Key expert 1. Backend senior software developer:
The senior software developer shall oversee that all reporting obligations are fulfilled in a timely manner to a high-quality standard.

- University degree in Computer Science or another relevant domain
- At least 5 years of experience in software development
- 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
- Participated in at least 2 software development projects in the last 3 years using agile approach
- Ability to communicate in Romanian or English

Key Expert 2. Backend/Frontend software developer:

- University degree in Computer Science or another relevant domain
- At least 3 years' experience in software development
- At least 2 years of experience in software development using any backend or frontend technologies (such as Angular, React or Vue)
- Certifications in any technology from the required technology stack is an asset
- Participated in at least one software development projects in the last 3 years using agile approach
- Ability to communicate in Romanian or English

Key expert 3. Android senior software developer:

- University degree in Computer Science or another relevant domain
- At least 5 years of experience in software development of native Android apps
- At least 2 years of experience in software development using Kotlin
- Familiarity with JetPack Compose framework is an asset
- Certifications in any technology from the required technology stack is an asset
- Participated in at least 2 software development projects in the last 3 years using agile approach
- Ability to communicate in Romanian or English

Key Expert 4. Android software developer:

- University degree in Computer Science or another relevant domain
- At least 3 years of experience in software development of native Android apps
- At least 1 year of experience in software development using Kotlin

- Familiarity with JetPack Compose framework is an asset
- Certifications in any technology from the required technology stack is an asset
- Participated in at least one software development project in the last 3 years using agile approach
- Ability to communicate in Romanian or English

Key expert 5. iOS senior software developer:

- University degree in Computer Science or another relevant domain
- At least 5 years of experience in software development of native iOS apps
- At least 2 years of experience in software development using Swift
- Familiarity with SwiftUI framework is an asset
- Certifications in any technology from the required technology stack is an asset
- Participated in at least 2 software development projects in the last 3 years using agile approach
- Ability to communicate in Romanian or English

Key Expert 6. iOS software developer:

- University degree in Computer Science or another relevant domain
- At least 3 years of experience in software development of native iOS apps
- At least 1 year of experience in software development using Swift
- Familiarity with SwiftUI framework is an asset
- Certifications in any technology from the required technology stack is an asset
- Participated in at least one software development project in the last 3 years using agile approach
- Ability to communicate in Romanian or English

Annexes

Annex 1. Business requirements

1. **Actors**

The following actors will be involved in MobiSign and will act in different capacities:

- **MobiSign Administrator.** A user of MobiSign performing technical administration tasks, acting on behalf of E-Governance Agency.
- **User Administrator.** An official state/private representative empowered to verify and register registrars of MobiSign system for its organization.
- **Registrar.** An official state/private representative empowered to verify the identity and register users of MobiSign system.
- **Support Operator.** A user that is empowered to review user devices and interactions (past authentications and signatures) to provide support on user's demand.
- **Verified User.** The verified and registered user of the MobiSign.

2. **Business requirements**

UC01: Registering of Users
Resident of the Republic of Moldova goes to the one of the approved registrars and present personal identification document (passport, ID card, driving license). Registrar fills-in the personal identification number into the solution back-end interface and receives up-to-date identification data from the National Registry of Population. Verifies the received data with the date from the provided ID and in case there are no discrepancies prints the pre-filled request for registration at MobiSign and gives it to the solicitant for reviewing and signature. After the solicitant signed the printed request for registration at MobiSign, registrar confirms request signature by signing the registration request. Solicitant will download the appropriate version of the app, launch it and enter or scan the registration code provided by registrar to initiate keys generation and registration in MobiSign infrastructure as well as PIN setup.

UC02: Signing into the MPass
Once registered, users shall be able to authenticate via MPass. Note that MPass changes required for this are not part of the assignment. To authenticate, a Registered User accesses MPass interface. From the proposed methods of signature selects MobiSign, inputs IDNP (national personal identification number) and press Send to initiate authentication flow. MPass computes the 4-digit verification code and MobiSign App notifies user on the registered device about authentication request. User reviews the verification code, provides PIN for authentication approval into MobiSign app interface. After MobiSign finalizes the authentication process, MPass receives authentication confirmation.

BR01: Registering of User Administrator
System administrator will be able to register User Administrators, delegated by an organization with registrar rights using MPass.

BR02: Registering of Registrars
User Administrator will be able to register and manage Registrar's accounts within organization using MPass.

BR03: PKI Integration
MobiSign backend component shall be ready to integrate with national PKI for certificate issuance and validations.

BR04: HSM Integration
MobiSign backend component shall be ready to integrate with HSM APIs for public key retrieval and using private key for signature.

Annex 2. Technical requirements

1. Documentation requirements

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 • Human and machine-readable description in a standard description language (e.g. WSDL or Swagger). All API documentation will be provided in English.

2. Rights requirements

Perpetual software license	The Consultant grants to the Client the rights to develop, 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 elsewhere.
Full data rights	The Client keeps full rights on data created by the means of this solution.
Open data format	The solution preserves 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 into another system.

3. 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 prototype shall be designed to 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.
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	MobiSign shall implement API to be consumed by governmental platforms MPass 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 Client in advance.

4. System Performance requirements

Asynchronous processing	System shall use asynchronous processing whenever possible to perform any input-output.
Concurrent users	The system standard load and performance shall be guaranteed for 100 concurrent human users.
Concurrent system requests	The system shall be designed to respond (via API requests) to at least 1000 concurrent external system requests.
Application performance	Mobile applications shall respond immediately or provide progress indication for long operations (for example keys generation).
Response time	Response time for server-side calls 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 shall be designed to process at least 1.000.000 transactions per day.

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.

5. User Interface requirements

Multilanguage User Interface	The system shall support multilanguage user interface. This support includes data type specific formats (such as date, time, time spans, etc.). The system front-end interface will be delivered with at least Romanian, Russian and English interfaces. The system back-end shall be delivered at least in Romanian and English. The default language for User interface shall be the Romanian.
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.
Contextual help	User Interface elements shall include Tips and Hints for user interface elements.
Client support	All pages shall include client support contacts.
Friendly URLs	MobiSign shall use friendly URLs for accessing its pages.

6. 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.

7. 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 Client 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.
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.
Users' roles management	The users and their roles will be managed in MPass. The system shall retrieve the users' roles from MPass.
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 minutes.

Authorized access to personal content	Users are granted access to content designated as belonging to them. Content belongs to a user if it has been assigned/addressed to their personal IDNP.
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 or alteration of notifications directly from database).