Terms of Reference

Development of the eKYC platform and integration with third party identification services

Development and Implementation

Contents

1 Introduction

The rapid advancement of digital technologies has fundamentally transformed interaction between individuals, businesses and public authorities, making services and internal processes more efficient, transparent, and accessible to citizens and businesses.

A critical element of this digital transformation is digital identity, which serves as the foundation for secure online transactions.

In Moldova, implementing a national reusable Electronic Know Your Customer (eKYC) solution as part of Digital Public Infrastructure (DPI) represents a strategic opportunity to streamline identity verification, reduce costs and enhance security. By leveraging access to state registries and other reliable data sources, the cutting-edge technologies as services and the expertise of qualified specialists, a reusable national eKYC solution can provide robust and efficient identification and verification mechanisms for both public and private sectors.

The World Bank Group provides continuous support to the Government of Moldova through consistent financing and technical assistance for the digitalization of the G2B services and digital transformation in general. The digitalization component of the Medium, Small and Medium Enterprise Competitiveness Project (hereinafter MSME) started in 2023 focuses on key activities related to expanding the digitization of Government-to-Business (G2B) services at the national and local levels, improving and digitizing inspection services, improving interoperability and integrated service delivery for businesses, and simplifying the regulatory environment to reduce regulatory burden.

Remote identification and onboarding are crucial components of digital transformation in Moldova, enabling facilitated access across e-Government solutions, financial and notarial services, healthcare, education and more. However, with rapid evolution of fraud techniques, including real-time deep fake video generation and synthetic identity fraud, there is a pressing need for secure, adaptive and scalable identity verification solutions. The proposed eKYC solution will: (i) enable businesses, investors, and public institutions to perform secure remote identification; (ii) enhance user experience by eliminating redundant identity checks across different services; (iii) reduce operational costs for services providers while ensuring compliance with regulatory requirements; (iv) increase security and fraud detection by integrating AI-powered liveness checks and biometric verification; (v) enable digital economy and new e-Government initiatives forming a new key component of national digital infrastructure.

In short, the proposed eKYC solution is a custom integration of:

- actively developed and evolving external services for advanced liveness, document and face match checking, adapted to evolving threats,
- national authentic data sources for evidence verification (such as State Registry of Population, etc.),
- other external services that can provide additional evidence collection and verification,
- a risk-scoring mechanism that can combine the above for an informed decision.

As technology progresses, the owner of the solution shall be able to continuously adapt it by integrating more external services and new data sources, and to actively maintain those integrations, as detailed in the **Strategy** section of the ToR.

The eKYC platform will be designed for scalability and adaptability, focusing initially on financial institutions, public notaries and public agency's needs (i.e., digital public services), but will also subsequently support telecom, healthcare, and other sectors. Relying parties (i) will integrate with the solution to trigger the remote customer identification process as part of their business processes, (ii) customers will interact with the eKYC solution's web or mobile components integrated into relying parties information systems in a wizard-like interface to provide evidence about their identity, (iii) the solution

validates and verifies the collected evidence and calculates the combined score to determine if identification process passed the configurable use case threshold, ensures proofs are recorded, and in the final step (iv) returns the identification result to the relying party information system, as described in the **Process Overview** section of the ToR.

One of the key strengths of the eKYC solution that will be used by many stakeholders is the feedback that it will provide to all of them. When an applicant makes their first physical contact with any stakeholder within the ecosystem, the outcome - be it positive or negative - can be shared and utilized to further enhance and refine the overall eKYC process. This continuous feedback loop strengthens the security and effectiveness of the solution, benefiting all stakeholders involved.

The deployment of the platform will be phased, ensuring flexibility, stakeholders' engagement, and regulatory alignment. The system will be designed to seamlessly integrate into the Moldova digital ecosystem, and first of all with the Governmental digital infrastructure elements such as MCloud, MConnect, MLog, MPay, MNotify, MPass, MSign and EVOSign.

The scope of this document is to describe the technical reasoning and requirements behind such a reusable national eKYC solution.

1.1 Acronyms and Definitions

The following acronyms are used in this document:

Acronym	**Definition**
API	Application Programming Interface
EGA	E-Governance Agency / organization
eKYC	Electronic Know Your Customer
HA	High Availability
HTTPS	HyperText Transfer Protocol Secured
IAL	Identity Assurance Level
ITSEC	Information Technology and Cyber Security Service / organization
JSON	JavaScript Object Notation
MVP	Minimum Viable Product
NFR	Technical or Non-Functional Requirement
RIDP	Remote Identity Proofing Provider
RP/SP	Relying Party or Service Provider – the party that requests for remote identity proofing
OIDC	OpenID Connect
OS	Operating System
REQ	Business Requirement
REST	Representational State Transfer
SAML	Security Assertions Markup Language
SDD	Software Design Document
SOAP	Simple Object Access Protocol
TLS	Transport Layer Security
ToR	Terms of Reference
WS	Web Services
WSDL	Web Services Description Language
XML	Extensible Markup Language

The following definitions are used throughout this document:

Definition	Description
Applicant	Person whose identity is to be proven
Attribute	Quality or characteristic ascribed to a person
Auditor	Authorized user of the system that can access data for auditing purposes.
Beneficiary/Owner	In context of this document the Beneficiary/Owner is EGA.
Claim	A particular information about natural person.
Client	World Bank's Project Implementation Unit - the organization managing the contracting and finances for this acquisition.
Consultant	The company that will provide this solution.
Evidence	Information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct.
Operator	Authorized user of the system that has the responsibility to verify data in scenarios requiring that.
Permissive documents	Means permits, licenses, approvals and authorizations
Verified Claim	An attribute who's binding to a particular person's identity was verified during an identity verification process

1.2 Goal

The main goal of the envisioned national eKYC solution is to deliver a reusable, secure and user-friendly identity verification process for various use cases and requested level of assurance.

The goal of this ToR is to describe the requirements for the implementation of the eKYC solution as an integration of external liveness, document and face match check services with platform services and other data verification sources.

The eKYC solution is a service run by E-Governance Agency (EGA) that enables relying parties to perform remote customer identification as part of their business processes. In technical terms, relying parties' information systems will integrate the identification subprocess through solution's APIs, web redirection to solution's web interface and by incorporating solution's mobile components into their mobile apps. After proper identification, the solution will persist the collected evidence in an auditable manner and securely return the results to the relying party.

1.3 Concept

Electronic Know Your Customer (eKYC) is a digital identity verification process that enables organizations to authenticate the identity of their customers in a secure, efficient, and user-friendly manner.

By leveraging advanced technologies, a national eKYC solution will streamline the identity verification for customer onboarding process and help governments and businesses address security concerns and meet regulatory compliance requirements in a cost-efficient manner.

The reusability aspect of a national eKYC solution is a key success factor, providing numerous benefits for both users and stakeholders. By creating a solution that enables secure sharing and reusing verified identity data, efficiency and trust in digital transactions will be significantly improved:

- **Streamlined Processes:** Once an applicant's identity is verified through the eKYC solution, their information can be securely shared with other participating entities in the ecosystem. This eliminates the need for applicants to repeatedly submit their personal data and undergo multiple verification processes, saving time and resources for both applicants and service providers.

- **Enhanced User Experience:** Reusability of eKYC output ensures a smoother and more convenient applicant experience. With their identity data readily available, applicants can access diverse services quickly and effortlessly, without having to undergo redundant verification procedures.
- **Reduced Operational Costs:** By eliminating the need for repetitive identity verification processes, businesses and service providers will significantly reduce their operational costs. The reusable eKYC solution allows organizations to focus on providing their core services, rather than investing in time-consuming and costly identity verification procedures.
- **Improved Security:** A reusable eKYC solution promotes a higher level of security and data protection. By consolidating identity verification in a centralized solution, the risk of data breaches and identity theft is reduced. Furthermore, the solution will be consistently updated with advanced security measures to ensure the utmost protection of applicant information.
- **Regulatory Compliance:** Implementing a national eKYC solution enables businesses and service providers to comply with evolving regulatory requirements more easily. As the eKYC solution adheres to stringent identity verification standards, participating entities can be confident in their compliance with relevant regulations and guidelines. At the same time, the eKYC solution implemented by EGA through this assignment does not exclude similar solutions developed by the alternative providers of similar tools, if they intend to make their own investment.
- **Interoperability:** The reusable eKYC solution fosters interoperability between different service providers and sectors. By creating a standardized and centralized platform for identity verification, seamless data sharing between various organizations and industries becomes possible, paving the way for the development of new partnerships and collaborative efforts.

By focusing on the reusability aspect of the eKYC solution, stakeholders can harness these benefits to create a more efficient, secure, and user-friendly digital ecosystem. This approach not only enhances the overall experience for users but also fosters collaboration and innovation among participating entities.

1.4 Strategy

As technologies advance at an accelerated pace and new national and international data sources become available for validation, the solution shall **continuously evolve and be actively developed by its owner,** in this case the EGA.

This means that various identity validation and verification modules would evolve and change their risk factor depending on evidence availability and validation credibility.

This also means the owner shall not be locked into any service provider and shall always have the possibility to adapt/further develop the solution by itself or with any external/integration service provider. As the owner has relevant experience and credibility in developing and maintaining solutions using a particular technology stack, that can be leveraged as an opportunity to achieve the vendor neutral approach mitigating the risks of vendor lock-in that is requested as one of the key success factors of this assignment. That basically means that the solution is a custom-developed information system that integrates evolving external services and data sources.

Reviewing several eKYC, remote identification and identity assurance implementations, as well as ENISA Attacks & Countermeasures study, it appears that the most technology heavy and, at the same time, one of the core secure differentiators of such solutions are the liveness, document and face match checks. As these checks are often provided as-a-service and each implementation might be using a different technology stack, it is envisioned that the eKYC solution will technically integrate the liveliness and document check functionalities as external services.

This approach would enable the best out of two worlds, the custom developed eKYC module added to the DPI that will ensure data protection, and the use of external services for liveliness and document checks allowing the portability. Keeping the internal developed custom solution for the eKYC solution under the

control of EGA as an owner will retain the owner's capability for adaptation and engaging necessary external services allowing the private sector innovations.

The implementation will integrate with existing external liveness, document and face match check services, identified by EGA as a result of a market research under a separate public procurement exercise. Such services might include additional checks (such as VPN use checking) that might be leveraged by the implementation. The integration will comprise server-side service integration and client-side user interface components integration. For auditability, the services provided should collect evidence and/or proof of external services interaction.

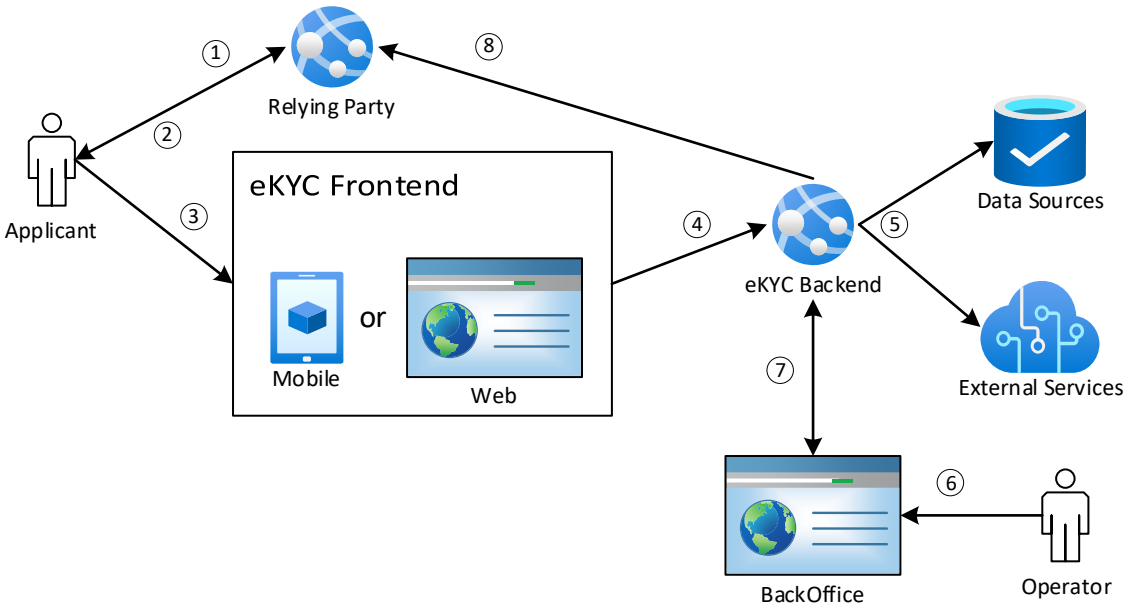
The Consultant shall be ready to integrate with external services proposed by the Beneficiary. The subscription to external services will be ensured by the Client.

1.5 Key Stakeholders

In line with the above-described goal and implementation strategy for the eKYC solution, the following is the list of key stakeholders that shall be involved in the development and implementation:

1) **E-Governance Agency** – product owner and main stakeholder, owner of EVOSign (which is the first and primary consumer of the solution), MPass (authentication and access control service) and MConnect (data exchange solution providing important data for the process).
2) **ITSEC** – main infrastructure provider for the solution and call center provider for operators, owner of MCloud.
3) **National Bank of Moldova** – the central banking authority which plays a crucial role in the financial sector development and openness to technological innovation. In the context of a reusable eKYC solution, the National Bank acts as a regulatory body, providing guidance and oversight to ensure its applicability by financial institutions according to international and national AML (Anti-Money Laundering) regulations.
4) **Public Services Agency** – as one of the main sources of data for evidence verification, such as basic person information, history of photos and documents.
5) **Public Service Providers** – various public institutions that provide non-electronic and electronic services requiring proof of identity. A reusable eKYC solution will help them provide their services remotely for users that do not possess an electronic identity or other means to prove their identity.
6) **Private Service Providers** (financial institutions, telecom operators, etc.) – various private entities that provide services requiring identity proof. A reusable eKYC solution will help them with customer onboarding in a cost-efficient and secure manner.
7) **Public Notaries** – legal professionals who provide authentication and certification services, such as witnessing and verifying signatures on documents, administering oaths, and certifying the authenticity of copies of original documents. In the context of a reusable eKYC solution, notaries will use the system to verify the identity of individuals involved in various transactions, thereby enabling remote delivery of their services.

1.6 Process Overview



The eKYC process is comprised of the following steps:

- **(1)-(2) Initiation** is the process of a Relying Party (RP) requesting for a remote identity proofing process because of the applicant requesting a service. The request shall include necessary information for tailoring to a particular service use case and identity assurance level. It shall be clear what evidence is mandatory to be collected, what can be skipped or if there are alternatives in the case where the applicant does not have certain evidence available.
- **(3)-(4) Attribute and evidence collection** is the process of applicant interaction with a front-end, which is a mobile app installed on their smartphone or web application accessed through a web browser, to enter (fill in a form, scan, sign, picture, or video record, etc.) the attributes and evidence.
- **(5) Attribute and evidence validation** is the process of validating the collected attributes against the provided evidence and ensuring the evidence is genuine and valid. This includes data checking and advanced analysis using available data sources and external services.
- **(6)-(7) Binding and verification** is the process of ensuring that the applicant presenting the evidence really is the person identified by the evidence.
- **(8) Issuing of proof** is the process of creating reliable evidence of the identity proofing process to be able to prove in retrospect why the identity proofing process yielded the given identity proofing result. The proofs are sent to RP for evaluation and further service offering.

Depending on the use case and evidence collection, validation or verification process, the process might be repeated in several iterations for steps (3) – (7).

1.7 Principles

Solution implementation will be based on the following principles:

- **Flexibility** – based on the use cases, the level of required assurance and applicant ability to prove claims, the solution dynamically defines the process of identity verification.
- **Continuous Improvement** – due to expected technological and regulatory evolutions resulting in emerging challenges or opportunities, the long-term success of the solution can be ensured by implementing various verification and validation processes as extensible and continuously maintained modules, both on client and server sides.
- **User-Friendliness** – solution should prioritize applicant experience, ensuring that the identity verification process is smooth, convenient, and inclusive, involving the creation of an intuitive

interface, minimizing the steps required for verification, and providing clear instructions and support for applicants throughout the process.

- **Privacy** – the solution must uphold the highest standards of security and data privacy to protect applicants' sensitive information and maintain trust in the system including robust encryption, access controls, and compliance with relevant data protection regulations.
- **Auditability** – the solution must preserve the received information from applicants and data sources in a manner that can be proven as authentic, by maintaining clear and comprehensive audit trails that track and record all activities and transactions.
- **Legality** – the solution must follow the legal framework that forms the basis for its implementation according to Annex 2.
- **Interoperability** – the solution will maximize its reusability by exposing and consuming standards-based integration interfaces.
- **Scalability** – the solution should handle a growing number of users and transactions over time without significant degradation in performance.
- **Resilience** – the solution should be designed to withstand and recover from various failures, such as hardware, system failures, and other disruptions.
- **Non exclusiveness –** the solution is provided to the market for use in a wide range of contexts and services, not excluding similar tools being the free choice of the service providers.

1.8 Deliverables

The Consultant shall provide the following deliverables during the course of this assignment:

1. **A fully functional and reusable eKYC solution**, developed in accordance with the requirements defined by the Beneficiary. The solution shall be deployed in both **staging and production environments**, and shall include all agreed functionalities. The Consultant shall deliver **complete, consistent, and compilable source code**, including:
    a. Unit tests.
    b. Automation scripts.
    c. Third-party tools and libraries (with licenses, where applicable).
    d. Technical documentation embedded within the codebase.
2. **Integration with third-party services** for **liveness detection, document verification, and face match checks**, based on APIs and providers separately identified and procured by the Beneficiary. The Consultant is responsible for ensuring correct integration and handling of these services within the eKYC workflows.
3. **Comprehensive test reports**, including results of **functional, performance, and security testing**, developed in accordance with the approved test plans and acceptance criteria.
4. **Technical documentation** and **end-user documentation**, prepared in line with the Beneficiary's requirements, covering system architecture, deployment, configuration, usage, and maintenance procedures.
5. **Training sessions and training materials**, designed and delivered in accordance with the Beneficiary's training plan, to ensure the effective use and administration of the eKYC solution by designated personnel.

1.9 Standards

The Consultant shall ensure that the design, development, implementation, and operation of the eKYC solution are fully aligned with internationally recognized standards and best practices. These standards shall guide all aspects of the software lifecycle, from architecture and coding to integration, testing, security, and interoperability.

1. Software Development Lifecycle

The project shall follow a structured and traceable software development lifecycle (SDLC), based on one or more of the following international standards:

- ISO/IEC 12207 – Software Life Cycle Processes
- ISO/IEC 15288 – System Life Cycle Processes
- ISO/IEC 21500 – Project Management Guidelines

The selected methodology shall support iterative development, continuous quality assurance, risk management, stakeholder engagement, and requirement traceability. The Consultant shall define and document the chosen SDLC model during the inception phase and apply it consistently throughout the project.

2. Information Security and Application Security

The solution shall incorporate secure development practices and robust security controls to protect personal and biometric data throughout its lifecycle. Compliance shall be ensured with the following standards:

- ISO/IEC 27034 – Application Security Techniques
- ISO/IEC 15408 – Common Criteria for Information Security Evaluation
- OWASP Top 10 – Web Application Security Risks
- OWASP Mobile Top 10 – Mobile Application Security Risks

Security measures shall include threat modeling, code-level security reviews, encryption of data at rest and in transit, secure session management, and protection against common application vulnerabilities.

3. Biometric and Digital Identity Standards

- Given the nature of the eKYC system, which relies on biometric identification and identity verification, the development team should ensure that, together with the integrated third-party services, the final solution adheres to specialized standards, as also outlined by the National Bank of Moldova:ISO/IEC 30107 – Biometric Presentation Attack Detection (PAD)
- ISO/IEC 24745 – Biometric Information Protection
- NIST SP 800-63 – Digital Identity Guidelines
- NIST SP 800-63B – Authentication and Lifecycle Management

4. Interoperability and API Standards

The solution shall ensure secure and standards-based interoperability with third-party services and external systems. Specifically:

The system shall implement OpenID Connect Verified Claims for identity verification requests and issuance of verified identity attributes.

It shall consume and expose APIs using REST/JSON and SOAP/XML, with support for the WS-Security framework where applicable.

All communication shall use HTTP/2.0 and TLS 1.3 or higher, with or without client certificate authentication, depending on integration needs.

Except for OpenID Connect endpoints, all exposed APIs shall follow REST/JSON over TLS with client certificate authentication and shall be documented using OpenAPI 3.0 or higher specifications.

The Consultant shall provide documentation, testing evidence, and implementation details to demonstrate how the above standards have been addressed. Any deviation from these standards must be explicitly documented, justified, and approved by the Beneficiary.

2 Timeline

The tasks defined under the current Project are estimated to be performed in 24 months of which 12 months for development and 12 months for the post-implementation support and warranty.

The active development phase of the project shall be organized according to the **Project milestones**.

The development team shall provide 12 months of warranty for the developed solution. More on warranty requirements can be found in the "Technical requirements" section of this document.

If new functionalities are identified by the Product Owner during the warranty period, these functionalities may be implemented in additional iterations (sprints), upon availability of budget.

3 Project Governance

3.1 General Provisions

The Consultant's software development team will be responsible for designing, developing, configuring, and deploying the eKYC solution as a fully functional product with all functionalities in place, according to the specifications iteratively defined by the EGA.

Due to the relative complexity of the eKYC, an iterative development approach is required to deliver the project on time and according to beneficiary's expectations. When developing the project implementation plan, the selected software development team shall consider the following organizational requirements:

- Development shall be based on an iterative development methodology.
- Each release plan is developed by the Consultant by taking features with topmost priority in the product backlog, which is maintained by the EGA. The release plan shall be approved by the EGA before starting the iteration.
- Each iteration shall result in a functional increment (release) of the solution to the pre-production environment.
- Each iteration shall end in a demo to EGA of the delivered functional increment.
- Prior to the start of the development, the EGA reserves the right to evaluate and approve the key experts, which will be involved in the eKYC development. Any changes to the key experts shall be notified with EGA and new team members shall be pre-approved by EGA before embarking on the project.

3.2 Institutional Arrangements

The Beneficiary is responsible for administrative and procedural aspects, including acceptance of deliverables/reports expected under the Contract, general project responsibilities and efficient coordination with stakeholders. The responsibility for supplying any legal expertise or procedural assessments needed when implementing laws and procedures through digital tools, including those related to the e-KYC purely relies on the Beneficiary and on the Secretariat of the Economic Council under the Prime Minister Office. Contract and financial management will be handled by the Client, which is World Bank's Project Implementation Unit, subject to the Beneficiary's approval.

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

The Beneficiary provides the following:

- computational resources for development, staging and production environments. The Consultant shall not include any hardware in its proposal;
- code repository, issue tracking system, CI/CD environment, task management system via the Beneficiary's subscription in Azure DevOps. The Consultant shall not include Azure DevOps subscription in its financial proposal;
- training facilities.

The Consultant ensures that adequate working conditions if necessary (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 will propose the initial eKYC Backlog. All Consultant's Key Experts as specified in the section defining the qualification requirements, shall participate in the Kick-off meeting (on site or on-line) and preparation of the initial eKYC Backlog.

The Consultant will ensure visits to the Beneficiary site to provide training for authorized users, such as Administrators, Operators and Auditors.

In case the deliverables contain defects and/or there are delays for reasons not imputable to the Beneficiary that may impact project outcome, the Consultant may be requested to visits to Beneficiary's site 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.

3.3 Reporting Requirements

The following reports will be provided during the assignment:

1) Sprint Report, including release notes, breakdown and duration of tasks implemented during the sprint, velocity, issues and outstanding problems, proposed actions to be taken;
2) 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 Beneficiary and/or actions to be taken by the Beneficiary;
3) Training reports, submitted after each training session, including:
    a) Participants list;
    b) Training session agenda;
    c) Training materials (presentations, labs etc.);
    d) Trainees test results.

3.4 Iterative development

The project will be managed using a **dual approach**, combining a **phased implementation structure** with **Agile delivery principles**. While the project is organized into clearly defined **milestones** (as described in section 4.5), each milestone will be executed through **Agile iterations (sprints)** that deliver functional increments of the solution.

Implementation will proceed through **successive phases**, with each phase corresponding to a milestone that includes a specific set of functionalities, documentation, and acceptance criteria. The deliverables for each phase will be defined in advance and validated upon completion.

Payments will be tied to milestone outcomes and will be issued only after formal acceptance of the corresponding deliverables by the Beneficiary, based on the agreed acceptance criteria for each phase.

3.5 Project milestones

Product Backlog and iterations will be organized in the following project milestones for the active phase of the project:

Documentation milestone that will result in a Software Design Document (SDD). This initial milestone is focused on establishing a shared understanding between the Consultant and the Beneficiary regarding system architecture, technical direction, and core processes. It will result in the development of a comprehensive Software Design Document (SDD), which will include identified system actors and use cases, logical architecture and components, process diagrams, wireframes for key user interfaces, technical implementation details, and deployment architecture. Additionally, the SDD will include an initial threat analysis and a description of the proposed security controls. As part of this milestone, the Consultant will also complete the setup of the development environment, including granting access to the Beneficiary's infrastructure, initializing the codebase and version control system, configuring the CI/CD pipeline, and preparing a standardized project template. The Consultant will work jointly with the Beneficiary to conduct backlog refinement sessions and validate design assumptions.

MVP milestone

During this phase, the Consultant will implement the full remote user enrollment workflow, including electronic document verification, facial recognition, and liveness detection, supported by secure evidence collection and storage. The solution will be integrated with the initially provided third-party services for document check, face match, and liveness verification. A minimal but functional version of the mobile application for Android and iOS will be developed to enable basic user flows. The Consultant will also deliver the initial version of external integration APIs to allow interoperability with client systems. Basic authentication and role management will be implemented to support MVP functionality. A demonstration environment will be set up and made available to the Beneficiary for iterative validation and feedback.

Extended Features milestone

The third milestone will focus on completing the remaining scope as defined in the backlog and functional specifications. During this stage, the Consultant will implement configuration management tools to enable dynamic rule-setting for different use cases. Additional types of evidence collection and validation will be developed, along with logic for binding and linking multiple evidence types. Integration will be completed with all required platform services, such as national registries, electronic identity, audit logging, and messaging systems. If applicable, logic for physical verification propagation will be implemented. The web-based administrative interface will be finalized with all necessary functionalities. The Consultant will also introduce enhanced error handling, comprehensive logging, and user-friendly fallback flows. Accessibility and responsiveness improvements will be applied to both mobile and web components, and final security hardening will be performed based on the updated threat model and consultation with the Beneficiary.

Acceptance milestone

The final milestone is dedicated to validating the solution against the agreed functional and non-functional requirements. This includes complete functional testing, performance testing, and security testing in a staging environment. Any issues identified will be resolved, and final refinements applied to ensure the solution meets quality standards. The Consultant will prepare and deliver all required documentation, including user manuals, system administration guides, API documentation, and updates to the technical

design documentation. Training sessions will be conducted for relevant staff designated by the Beneficiary. The Consultant will support User Acceptance Testing (UAT), incorporate feedback, and finalize go-live planning. All deliverables will be subject to approval before operational handover.

The Consultant shall deliver the eKYC solution using a **well-defined and structured software development lifecycle (SDLC)** aligned with internationally recognized standards. The selected lifecycle shall follow established frameworks such as **ISO/IEC 12207** (Software Life Cycle Processes), **ISO/IEC 15288** (System Life Cycle Processes), or **ISO/IEC 21500** (Project Management Guidelines). The chosen methodology shall be specified during the inception phase and must support iterative delivery, quality assurance, traceability, stakeholder involvement, and risk management throughout the development process.

The Consultant shall demonstrate through technical documentation, implementation practices, and testing that the system design incorporates the principles and controls required by the required standards. This includes, but is not limited to, biometric data protection, anti-spoofing mechanisms, secure authentication flows, privacy preservation, and application-level security. Any justified deviations must be documented and approved by the Beneficiary.

Payments will be made upon successful completion and acceptance of each milestone. The company must propose an implementation plan in the offer, including when the external services for liveness, document and face match checks must be provided, the proposed duration of the milestones and level of effort for key and non-key experts for each milestone of the project (12 months).

3.6 Working product in each iteration

Each sprint, post the Documentation milestone, shall result in a **Release Candidate (RC)**—a fully functional and production-quality version of the system increment—which will be presented to the Beneficiary for review and acceptance during the final day(s) of the sprint. The Consultant shall be fully responsible for conducting **end-to-end testing and validation** of each Release Candidate prior to its submission. This includes functional testing, integration testing, performance checks where relevant, and security validation of the delivered scope.

The Release Candidate must comply with the agreed **Definition of Done**, which includes: full functionality as per sprint backlog, successful completion of all planned and regression tests, coverage by relevant unit and integration tests, complete and clearly commented source code, and updated technical or user documentation where applicable. Only deliverables meeting all these conditions will be considered for acceptance.

In the event that any defects are identified in the deliverables that are not attributable to the Beneficiary, the Consultant shall correct them **at no additional cost** and **without impacting on the overall project schedule**. Where necessary, this includes on-site visits or direct coordination to resolve issues.

While each sprint delivers a Release Candidate, the decision to consolidate multiple increments into a formal production release remains at the sole discretion of the Beneficiary, based on internal priorities and deployment readiness.

Any incidents reported by the Beneficiary after the release shall be solved by the Consultant according to the 6.10 Warranty and support requirements NFR 10.01 - 10.02.

To ensure that the development team is in position to deliver on time working products, a Beneficiary representative – the Product Owner – is permanently available to the team for answering eventual questions, thus not slowing down the implementation pace. Product Owner will ensure the full involvement of the relevant Beneficiary representatives.

3.7 Beneficiary involvement

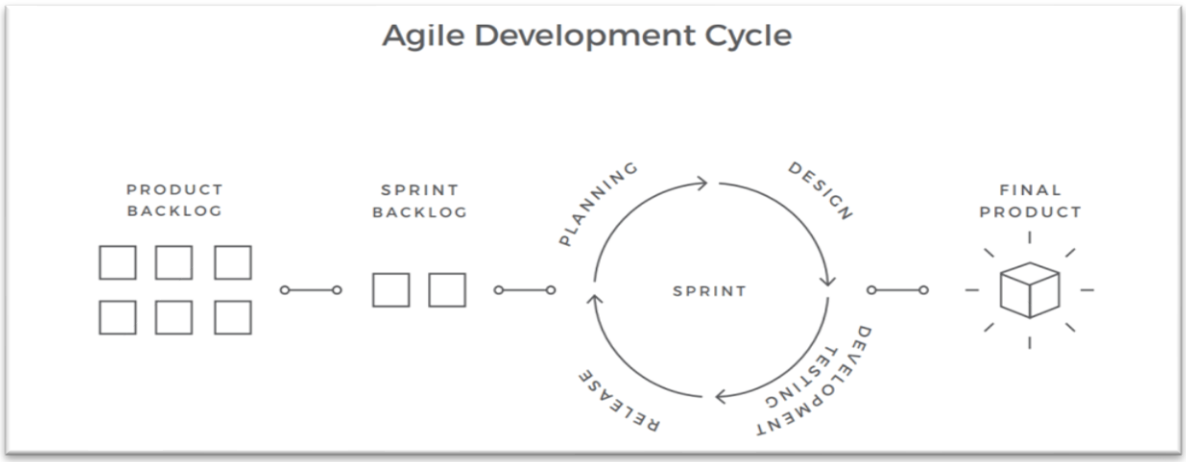
The Beneficiary shall appoint a **Product Owner**, who will act as the primary representative of the Beneficiary throughout the development process and will participate actively in all major stages of the project. The Product Owner will hold the following key responsibilities:

1. **Product Backlog Ownership:** The Product Owner is responsible for maintaining the product backlog, ensuring it remains up to date and reflects a clearly prioritized list of functionalities and requirements. The Product Owner will collaborate with the Consultant to refine backlog items and provide timely input on new or changing priorities.
2. **Support for the Development Team:** The Product Owner shall be available to the development team throughout the sprint to respond to clarification questions, provide guidance, and ensure alignment with the product vision. This direct and informal communication channel is essential to prevent delays and reduce unnecessary procedural overhead.
3. **Sprint Review and Acceptance:** At the end of each sprint, the Consultant will present the working package (Release Candidate) to the Product Owner for review. The Product Owner shall confirm acceptance or provide written feedback identifying any issues, bugs, or incomplete features during the following sprint. Acceptance of a working package does not remove the Consultant's responsibility to correct defects identified later, if they fall within the agreed Definition of Done or quality criteria.

While not mandatory, the Product Owner may also participate in team stand-up meetings to stay informed on progress and identify blockers early, enabling prompt decision-making and issue resolution.

In addition to these ongoing responsibilities, the Product Owner will also decide on the **approval and release of the MVP**, as well as any subsequent releases to the production environment, in accordance with the project's release strategy.

As part of Agile project management principles, the Beneficiary shall define the **Product Vision Statement** and maintain a **Product Roadmap** to guide development progress and ensure alignment with strategic objectives.



The indicative illustration of the Agile Development Cycle/Process.

3.8 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 Beneficiary

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:

1) Have been in operation for at least five (5) years with the main part of its business being the development of information systems.
2) Experience in conducting projects of similar size and complexity developing web applications and mobile applications with their backend proven by at least two (2) contracts (either both for mobile applications or one for mobile and the other for web application) with the development phase finalized in the last three (3) years. For ongoing projects, copies of acceptance documents of the entire software solution shall be provided.
3) Experience with implementing or integrating with eKYC-related technologies, such as implementation of a two-factor authentication provider, liveness check, biometric authentication, document match, face recognition, video processing, document OCR, MRZ recognition, etc.
4) Experience in software development using agile software development principles (as described in the scope of work and development approach section of the ToR), or following a well-defined software development lifecycle, such as based on ISO/IEC 15288, ISO/IEC 12207 or ISO/IEC 21500 standards, would be an asset. This shall be demonstrated by presenting the project methodology describing the roles of the Team and Beneficiary.

Key Experts qualifications requirements

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

- Key expert 1. Senior software developer.
- Key expert 2 and 3. Backend software developer.
- Key expert 4 and 5. Mobile software developer.
- Key expert 6. Software tester.

Each key expert must meet the **specific qualifications** outlined for their respective role (as described in the role requirements section). In addition, the following competencies will be considered as **desirable assets** across the team:

- Experience in implementing responsive UI/UX designs using modern web frameworks
- Experience in database design, development, and performance optimization
- Experience in system integration, API design, and development using SOAP/REST
- Experience in mobile development using Kotlin (Android)
- Experience in mobile development using Swift (iOS)
- Experience in unit testing and test automation
- Experience in secure coding practices, security testing, or code security reviews
- Experience in DevOps practices and tools
- Experience in system analysis and functional modeling

The composition of the team should ensure that these competencies are **collectively covered**, while each expert is demonstrably qualified for their assigned responsibilities.

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

Key expert 1. ***Senior software developer, Team Leader***:

The Senior Software Developer / Team Leader will be responsible for the technical oversight of the development process and will ensure that all deliverables and reporting obligations are met on time and

to a high standard of quality. This role combines strong hands-on coding expertise with leadership and communication responsibilities across stakeholders.

- University degree in Computer Science or a related field.
- Minimum 5 years of experience in software development.
- Demonstrated participation in at least 2 agile software development projects in the past 3 years.
- At least 3 years of experience in software development using:
    - C#
    - Entity Framework
    - ASP.NET Core
    - MS SQL Server
- Experience with Blazor web framework is an asset;
- Experience developing native mobile applications is an asset
- Experience working with technologies related to eKYC is a plus, such as:
    - Video capture and streaming,
    - Face matching / liveness detection APIs,
    - ID document OCR and verification tools;
- Familiarity with REST APIs, microservices architecture, and DevOps practices is highly desirable;
- Certifications in relevant technologies or cloud platforms (e.g., Microsoft Azure, .NET, SQL Server) are an asset.
- Proven experience in team leadership or coordination, including:
    - Task distribution and sprint planning,
    - Code review and quality assurance practices,
    - Coordinating with QA, DevOps, and product stakeholders;
- Strong reporting and documentation skills, including the ability to provide progress updates and technical documentation in line with project requirements;
- Excellent communication skills in Romanian and/or English, both spoken and written.

Key Expert 2 and 3. ***Backend Software developer***:

- University degree in Computer Science or a relevant field;
- At least 3 years of experience in software development;
- Participated in at least 2 software development projects in the last 3 years using an agile approach;
- At least 2 years of experience with:
    - C#
    - Entity Framework
    - ASP.NET Core
    - MS SQL Server
- Experience using the Blazor web framework is an asset;
- Experience working with technologies related to eKYC, video processing, or liveness detection is an asset;
- Familiarity with DevOps workflows, version control systems (e.g., Git), and branching strategies is a plus;
- Experience with microservices architecture, identity management, or message queues (e.g., RabbitMQ, Kafka) is a plus;
- Certifications in any of the technologies listed or relevant cloud platforms (e.g., Azure, AWS) are an asset;
- Strong collaboration skills and ability to work effectively within cross-functional teams;

- Accountability and clear communication in delivering estimates, technical input, and progress updates;
- Ability to communicate effectively in Romanian or English, both spoken and written.

Key Expert 4 and 5. *Mobile Software developer*:

- University degree in Computer Science or another relevant domain;
- At least 3 years of experience in mobile software development;
- Participated in at least 2 software development projects in the last 3 years using an agile approach;
- At least 2 years of experience in software development using **Kotlin** and/or **Swift**;
- Experience working with technologies related to **eKYC, video processing**, or **liveness detection** is an asset;
- Experience with camera access, biometric APIs, or device permission management is a plus;
- Familiarity with mobile app architecture patterns (e.g., MVVM, Clean Architecture) is a plus;
- Experience integrating mobile apps with secure REST APIs and identity/authentication flows is a plus;
- Certifications in any of the technologies listed or in mobile development platforms are an asset;
- Strong collaboration skills and ability to work in coordination with backend, QA, and design teams;
- Ability to communicate effectively in Romanian or English, both spoken and written.

Key Expert 6. *Software Tester*:

- University degree in Computer Science or another relevant domain;
- Minimum 3 years of experience in software testing planning and execution for projects of similar complexity;
- Proven ability to define and manage comprehensive test strategies, plans, and documentation for end-to-end testing cycles;
- Experience with manual exploratory testing, including edge-case validation and user scenario coverage;
- Proven experience in:
    - Software testing analysis and design;
    - Automated testing (e.g., Selenium, Cypress, Playwright, or similar tools);
    - Performance testing (load, stress) using tools such as JMeter, Gatling, etc.;
    - Security testing approaches and common vulnerabilities (e.g., OWASP Top 10);
- Experience in integrating automated tests within CI/CD pipelines (e.g., GitLab CI, Jenkins, GitHub Actions);
- Familiarity with test data and environment management, including creation and anonymization of datasets;
- Proficient use of issue tracking systems such as Jira or Azure DevOps, with clear defect reporting and traceability;
- Experience with documentation review and validation, including identifying non-testable or ambiguous requirements;
- Strong sense of ownership, with ability to work independently while collaborating effectively with developers, designers, and product managers;
- Excellent attention to detail and problem-solving skills;
- Experience with technologies related to eKYC, video processing, or liveness detection is considered an asset;
- Relevant certifications in software testing (e.g., ISTQB) or related technologies are considered an asset;

- Fluency in Romanian or English (spoken and written).

The Consultant shall designate a **Scrum Master**, selected from among the team of key or non-key experts, to serve for the entire duration of the project.

The **Scrum Master** will be responsible for:

- Acting as the **primary liaison with the Beneficiary** on all matters related to daily coordination, progress, and issue resolution;
- Facilitating **internal coordination among project experts**, ensuring effective collaboration, information flow, and task execution;
- Ensuring **alignment between the development team and external counterparts**, including stakeholders and third-party contributors;
- Leading agile ceremonies such as sprint planning, daily stand-ups, sprint reviews, and retrospectives;
- Monitoring sprint execution and addressing blockers to maintain delivery timelines;
- **Ensuring the availability and timely engagement of appropriate experts** in accordance with the approved project work plan and resource schedule;
- Supporting documentation of sprint activities and ensuring deliverables meet quality and schedule expectations.

The Scrum Master must have strong communication and organizational skills, and prior experience managing agile teams in software development projects of comparable scope and complexity is highly desirable.

Non-Key Experts qualification requirements

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 have to be listed in the technical proposal and their rates indicated 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, other support activities, etc.) 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(s);
- Product manager;
- UX/UI designer
- DevOps specialist;
- Technical writer/BA.

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.

4 Business Requirements

This section includes business or functional requirements for the solution.

4.1 Configuration

The following solution configuration requirements apply:

Requirement	Description
REQ 01.01 Evidence configuration	The Administrator can configure collectable evidence implementation parameters, such as connection strings or other specific configuration parameters.
REQ 01.02 Use-case configuration	Administrator can configure use cases and associated identity assurance level with a list of applicable evidence with the following properties: 1. Evidence risk factor (additive or multiplicative) for the use case. 2. Whether evidence can veto the process, i.e., if the check is not positive, the process fails. 3. Whether evidence is mandatory or can be skipped. 4. Alternative evidence, ordered by priority, if applicable. 5. Minimum score threshold required for this use case.
REQ 01.03 Client configuration	Administrators can associate solution clients with applicable use cases and assurance levels.

4.2 Initiation

The following requirements apply to the initiation step of eKYC process:

Requirement	Description
REQ 02.01 OIDC Initiation	Process initiation shall use OpenID Connect protocol with verified claims extensions, optionally specified the purpose of the identity verification (use case) and the required assurance level
REQ 02.02 Dynamic process	Depending on the client, requested use case, and requested identity assurance level, the solution will build a plan for evidence collection, validation, and verification.

4.3 Collection

The following requirements apply to the attribute and evidence collection step of eKYC process:

Requirement	Description
REQ 03.01 Evidence availability	The applicant shall be asked for the availability of evidence. For example, if applicant doesn't have an electronic document that can be remotely checked, if not mandatory, the check will be skipped, and the resulting validation will continue and considered with higher risk.
REQ 03.02 Evidence alternative	If applicable, the applicant shall be offered evidence alternatives. For example, if an applicant cannot prove its mobile phone number via an OTP sent using an SMS, a phone call dictating the OTP might be suggested as an alternative.
REQ 03.03 Wizard	Applicant interface shall show a non-intrusive progress bar and act as a wizard during the evidence discovery and collection. It is OK for the wizard steps and progress to change depending on evidence availability.
REQ 03.04 Input validation	The solution shall perform input validation on both client and server sides.
REQ 03.05 Input hints	Whenever applicable, the solution shall show descriptive labels, hints, or tooltips for inputs.

Requirement	Description
REQ 03.06 Offline recording	When high video and/or audio recording quality is required, the solution shall be able to record it offline on applicant device and then submit it to the server preserving quality.
REQ 03.07 Online call	When live interaction is required (for example with an operator), the solution shall provide live video/audio streaming.
REQ 03.08 Online chat	When clarifications are required, the solution shall implement an online chat that includes basic texting, file sharing and presence, message delivery indicators.

4.4 Validation

The following requirements apply to the attribute and evidence validation step of eKYC process:

Requirement	Description
REQ 04.01 Combined score	Evidence validation shall combine the results of validation into a scoring and compare it with the use case threshold. If lower, an automatic decision might be taken or the operator(s) decision might be requested.
REQ 04.02 Data match	The solution shall be able to check the exact match of evidence with data retrieved from various data sources. Exact text match includes punctuation, case, and accent (diacritic) insensitive variants. To implement this in a generic way, irrespective of data source, MConnect offers pre-processed data in uniform format and using an agreed protocol. eKYC can query MConnect using unique citizen identifier (IDNP) to retrieve data from different sources, the only difference being the data retrieval operation that is called and specific response structure.
REQ 04.03 Partial data match	The solution shall be able to check partial match of evidence (partial text match, maximum distance between geographical coordinates, etc.) with data retrieved from various data sources.
REQ 04.04 Record validity check	The solution shall be able to check the existence or validity of a record in some data source. An example would be the check of existence of a document, its validity period, and its status (not lost, stolen, broken, misprinted, etc.).
REQ 04.05 Custom data check	The solution shall include the possibility to code or configure a custom logic for data checking. For example, having the applicant's country determined by its IP address, compare that with the history of applicant border crossings.
REQ 04.06 Face(s) match	The solution shall be able to check the face match of one photo compared to one or more other photos.
REQ 04.07 Face extraction	The solution shall extract a person’s face photo from the document’s photo. This shall be implemented by leveraging the provided external services.
REQ 04.09 Operator review	The solution shall include the possibility for offline operator review of presented evidence and automatically computed scoring (for each evidence and total). The operator shall be randomly selected.
REQ 04.10 Live operator	The solution shall include the possibility for live operator interaction with live video/audio and chat directly in the solution or using external communication channels. The operator shall be randomly selected.
REQ 04.11 Multi-operator	The solution shall include the possibility of multi-operator review of the evidence. The operators and their order shall be randomly selected.

4.5 Binding

The following requirements apply to the binding and verification step of eKYC process:

Requirement	Description
REQ 05.01 Auditability	The solution shall record the evidence involved in an auditable form. For example, if data sources provide data using electronically signed messages, the

Requirement	Description
	message shall be persisted including the signature. Obtained photos and videos are certainly part of the recorded evidence.
REQ 05.02 Capture applicant device	Recorded audit data shall include details about applicant device (OS, manufacturer, model, unique identifier), agent (OS, browser version), IP address, etc.
REQ 05.03 Tamper proof audit	The solution shall store audit data in a tamper proof way, including logging into MLog.
REQ 05.04 OIDC Result	The process shall end by returning verified claims data using OpenID Connect protocol and format. The result shall include a transaction identifier (for any investigations) and validated evidence details. The returned details are configurable, and applicant may choose not to send non-essential evidence to the RP.

4.6 Evidence

The following evidence collection and validation must be implemented in the solution:

Requirement	Description
REQ 06.01 Basic data	The solution shall be able to check basic person data entered by the applicant using the State Registry of Population.
REQ 06.02 Electronic Document Check	The solution shall be able to collect and validate document data according to ICAO DOC 9303. This includes MRZ scanning using camera (requires OCR capabilities) and NFC scanning for data extraction from the chip, traffic being encrypted with a key derived from MRZ. The scanning process shall include guidelines and be easy to follow for the applicant. The solution shall validate the data with Registry of Population, including for lost, stolen, expired and other appropriate flags for the verified document.
REQ 06.03 Document Check	The solution shall be able to collect and validate document data. This includes taking the picture of the document (with passive and active checks), matching it with a template document and extracting data (OCR). This check shall be implemented by leveraging the provided external services.
REQ 06.04 Face Check	The solution shall check the photo of the applicant with that from electronic or non-electronic document and with multiple photos available from State Registry of Population. This check shall be implemented by leveraging the provided external services.
REQ 06.05 Liveness Check	The solution shall check the liveness of the applicant. This check shall be implemented by leveraging the provided external services.
REQ 06.06 Electronic identity check	The solutions shall include electronic identity check, if available for the applicant. Passing some minimal identity checks, if applicant has an electronic signature, but declares he does not, this shall veto the whole validation process and start appropriate fraud check processes.
REQ 06.07 E-mail check	The solution shall include the possibility to check applicant's e-mail address using an OTP. The connection to SMTP server will be provided by EGA.
REQ 06.08 Location check	The solution shall include location match (available on mobile phones and browsers) with declared residency address. Approximate residency address coordinates shall be taken from Registry of Addresses.
REQ 06.09 IP address check	The solution shall include the possibility to check the country of applicant location based on its IP address. The solution might also check if the IP address is known to be assigned to a VPN service provider, resulting in increased risk of fraud.
REQ 06.10 Card Check	The solution shall implement banking card check by making a zero-amount transaction and validating applicant's first and last name. Integration details will be discussed during project implementation.

Requirement	Description
REQ 06.11 PSD2 Check	The solution shall implement applicant account validation using PSD2 Account Information Service. PSD2 is expected to be implemented in Moldova in 2025.
REQ 06.12 Phone number check	The solution shall include the possibility to check applicant's phone number, using an OTP delivered via an SMS or a phone call. The external service to be integrated with for this will be identified during project implementation.
REQ 06.13 Other checks	Additionally, the solution might implement the following additional checks: • Verify knowledge of details from utilities bills. • Verify physical mail access or address proximity by mailing a one-time passcode. • Check a confirming signature of the peer, that already successfully passed the eKYC process.
REQ 06.14 Auditor	The Auditor shall be able to search for and review any eKYC session, successful or failed, including collected evidence, performed checks and responses of external services.

4.7 Integration

The reusability of the solution as part of larger systems is enabled by the following integration requirements:

Requirement	Description
REQ 07.01 Web and Mobile clients	It shall be possible to integrate relying party's web and mobile apps as clients.
REQ 07.02 Mobile module	The solution shall provide a mobile module to be integrated withing another mobile app, using native technologies for Android (compatible with latest Kotlin-based apps using JetPack Compose) and iOS (compatible with latest Swift-based apps using SwiftUI). The Modules interface shall be brandable (colors and fonts), and the wizard's progress bar shall consider that the integrating app can have some preceding and following steps.
REQ 07.03 Mobile app	The solution shall include a stand-alone dedicated mobile app that implements remote identity proofing.
REQ 07.04 Web app	The solution shall include a web-based app that implements identity validation. The web variant would certainly be limited in evidence it can collect compared to a mobile app.
REQ 07.05 Physical verification propagation	The solution shall propagate the result of a physical verification of the applicant at any client. This notification shall be done in both positive and negative cases.
REQ 07.06 Logging events for billing	The system must log events with sufficient data to support billing, including at a minimum a reference to the customer and the amount of service provided. These events must be recorded synchronously and transactionally to prevent underbilling or duplicate billing.

5 Technical Requirements

This section includes technical or non-functional requirements for the information system implementing the solution.

5.1 Technology Stack

The following requirements apply to all components of the solution, except external services:

Requirement	Description
NFR 01.01 Server Technology Stack	To preserve EGA investments and leverage the reusable integration libraries, the solution shall be developed using the latest versions of the following technology stack: • The programming language is C#. • The ORM is Entity Framework Core. • The Web framework is ASP.NET MVC Core. • The UI component library is Blazor/MudBlazor. • The package manager for components is NuGet. • The RDBMS is SQL Server. • The container orchestrator is Kubernetes. • The installation shall be configurable and automated using Helm charts. • The caching server and session store, if used, is Redis. • The file or blob storage is MinIO.
NFR 01.02 Hosting in MCloud	Following the previous requirement, the solution will be hosted in governmental cloud infrastructure, called MCloud. This also means there shall be no hardware delivered as part of the implementation.
NFR 01.03 Mobile Technology Stack	Mobile modules and apps shall be developed using native technologies for Android (compatible with latest Kotlin-based apps using JetPack Compose) and iOS (compatible with latest Swift-based apps using SwiftUI). Libraries provided by 3rd party shall be used only when the direct manufacturer does not offer a standard implementation, or the standard implementation does not cover some requirements.
NFR 01.04 Browser compatibility	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.

5.2 Licensing and rights

The following requirements apply to all components of the solution, except external services:

Requirement	Description
NFR 02.01 Perpetual software license	The Consultant grants the Beneficiary the right to build, run and use the entire solution with all included software components with no constraints on time, location and offered functionality. If any licenses are required for this, the Consultant shall transfer or buy those licenses as unlimited and perpetual licenses in the name of the Beneficiary.
NFR 02.02 Redistribution rights	The Consultant shall grant the Beneficiary the right to re-distribute the solution.
NFR 02.03 Full data rights	The Beneficiary keeps full rights on data created by the means of this solution.
NFR 02.04 Open data formats	The solution preserves the data in open formats or includes mechanisms to extract data from the system in open formats thus enabling the capability to transfer/migrate the data into another system.
NFR 02.05 Detailed data model	The system's detailed data model shall be described fully in a machine-readable data scheme, for example using a DDL language for relational databases, or all classes and annotations in a code-first approach.

Requirement	Description
	Detailed data model schema format shall be coordinated with the Beneficiary.

5.3 Architecture

Requirement	Description
NFR 03.01 Open Standards	The system architecture shall be based on relevant open standards and specifications. The solution architecture shall not use proprietary standards. Besides standards listed in the document, any other protocols or formats shall be discussed during the implementation with the Beneficiary.
NFR 03.02 UTF	The system shall work with all Unicode character set, either UTF-8 or UTF-16 shall be used when handling strings.
NFR 03.03 UTC	The solution shall store all date and time data using UTC time zone, while users shall see them converted in their local time-zone.
NFR 03.04 Microservices	The solution shall be following Service Oriented Architecture principles and features that are coherent by their scalability, security or other requirements must be deployed as separate microservices.
NFR 03.05 Running environment	The system shall run as container instances and shall not depend on specific host OS instances. Building container images shall be automated.
NFR 03.06 Scalability	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.
NFR 03.07 Multiple sites	The solution architecture shall ensure high availability including during new versions deployment and the possibility to run simultaneously on multiple sites

5.4 Integration

Requirement	Description
NFR 04.01 Governmental platform integration	The system shall integrate with the following platforms: • MPass shall be used to authenticate and authorize users on the server-side. MPass shall also be used to authenticate client systems. • MSign shall be used to sign and verify electronic signatures. • MConnect shall be used to exchange data with data sources. • MLog shall be used to journal business critical events. The events that are business critical and will be sent synchronously or asynchronously will be defined at analysis and design stages and must be configurable. • MNotify shall be used for notifications. • MPay is used to request and accept payment.
NFR 04.03 Third party systems integration	The solution shall expose standard-based APIs for 3rd party systems integration.

5.5 Maintenance

Requirement	Description
NFR 05.01 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.). The logging framework shall minimally support JSON format and the following targets: console, rolling files, UDP and HTTP POST. Server-side logging shall use standard .NET ILogger interface.
NFR 05.02 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 errors that require human intervention. Event log records will include at least:

Requirement	Description
	• 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.
NFR 05.03 Open Telemetry	The system shall expose important business and technical metrics using Open Telemetry.
NFR 05.04 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.
NFR 05.05 Source code	The Consultant shall supply all the source code for system components that are not available as (C)OTS from third parties. The source code shall rely on package managers and public registries to declare 3rd party library dependencies. All prerequisite software must be part of container image definition and based on public container repositories.
NFR 05.06 System deployment	The Consultant shall supply the deployment procedure and supporting tools for this. The deployment procedure shall cover all the prerequisites before proceeding to system installation. The deployment shall be automated and include database structure initialization and seeding.
NFR 05.07 System upgrades	System upgrades shall be automated, including database upgrade/downgrade scripts or code and data migration. To enable rolling upgrades in production environment, the recommended practice is to perform database breaking changes in multiple increments.

5.6 Performance

Requirement	Description
NFR 06.01 Asynchronous processing	The system shall use asynchronous processing where feasible to handle input/output operations, including long-running or resource-intensive tasks.
NFR 06.02 Background uploads	Large file uploads shall be performed in the background, allowing the user to continue interacting with the system without interruption or performance degradation.
NFR 06.03 Concurrent users	The system shall ensure stable performance under a load of 100 concurrent remote enrollments and 10 simultaneous system operators. This load shall be sustainable for at least one hour without performance degradation.
NFR 06.04 Concurrent system requests	The system shall be designed to respond (via API requests) to at least 250 concurrent external system requests.
NFR 06.05 Response time	The response time for standard system functions shall not exceed 3 (three) seconds. Exceptions must be agreed upon with the Beneficiary during the analysis and design phases. For enrollment-specific processes, **95% of enrollment-related API calls must complete within 2 seconds**, and **end-to-end enrollment flows (from session initiation to verification result) must be completed within 60 seconds for at least 90% of users**. Notable exceptions may include media uploads and report generation, which shall be handled asynchronously.
NFR 06.06 Daily transactions	The system shall be designed to process at least 10.000 remote enrollments per day.

Requirement	Description
NFR 06.07 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 Beneficiary.
NFR 06.08 Resources estimate	The Consultant shall estimate and finally adjust the required resources from the hosting environment to cover the performance requirements.

5.7 User Interface

Requirement	Description
NFR 07.01 Multilanguage user interface	The system shall support multilanguage user interface. This support includes data type specific formats (such as date, time, time spans, currencies, etc.). The system will be delivered with at least Romanian and English interfaces. The default language shall be the Romanian.
NFR 07.02 User Interface Accessibility	User interface shall conform at least to Level A of Web Content Accessibility Guidelines 2.1. See https://www.w3.org/TR/WCAG21/
NFR 07.03 Responsive and Adaptive design	The system user interface shall automatically adapt to various display resolutions. Minimal display width is 480px. The web-UI shall be functional and usable on mobile devices.
NFR 07.04 Minimal User Flow	The system user interface shall minimize the number of clicks or taps for users to achieve the most used interaction scenarios.
NFR 07.05 Contextual help	User Interface elements shall include Tips and Hints for user interface elements.
NFR 07.06 Support	All system shall provide easy access to Beneficiary support contacts.
NFR 07.08 Bookmarks	Important system pages shall be bookmarkable, and the User shall be able to access bookmarked pages later.
NFR 07.09 Friendly URLs	The system shall use friendly URLs for accessing its pages.

5.8 Security

Requirement	Description
NFR 08.01 Secure by design	The system shall be secure by design and comply with the relevant requirements specified at Level 2 in GD 201 from 28.03.2017 (https://www.legis.md/cautare/getResults?doc_id=98644).
NFR 08.02 Security design documentation	The Consultant shall supply documentation describing design of security features and supporting evidence 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.
NFR 08.03 Least privilege principle	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.
NFR 08.04 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.
NFR 08.05 Secure communication channels	All system's communication with external systems or users takes place over encrypted communication channels. For public network communications, when both communicating parts are part of the solution, the system shall implement public key pinning with a clear change procedure.
NFR 08.06 Multi-factor authentication	The system shall rely on authentication via MPass. Other forms of user authentication shall not be used.

Requirement	Description
NFR 08.07 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.
NFR 08.08 Secure against OWASP Top 10 vulnerabilities	The system shall include security controls for all its components for at least OWASP Top 10 and be tested using MASTG with version applicable at the time of publishing the requirements. See https://owasp.org
NFR 08.09 Health-check API	The system components shall expose readiness and health-check API via 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.
NFR 08.10 Role management	The users and their roles will be managed in MPass. The system shall retrieve the users' roles from MPass.
NFR 08.11 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.
NFR 08.12 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.
NFR 08.13 Input validation	All input data shall be validated on client and server side.
NFR 08.14 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.
NFR 08.15 Data integrity	The system will ensure important data integrity by providing appropriate solution for prevention of unauthorized internal activities (for ex. Modification or deletion of records directly from database).
NFR 08.16 Mobile device and app integrity	The mobile module shall validate mobile device and application integrity during security-sensitive operations by using Google Play Integrity API and Apple DeviceCheck service.

5.9 Documentation and Training

Requirement	Description
NFR 09.01 User Documentation	The Consultant will prepare and deliver the following documentation for end-users: • Interactive guidance included in user interface adjusted to user role. • Editable user manuals in DOCX format by user role. All end-user documentation will be provided in Romanian.
NFR 09.02 How-To video tutorials	The Consultant will prepare How-To video tutorials for applicants.
NFR 09.03 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). • 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).

Requirement	Description
	• Maintenance plan, including monitored KPIs, planned tasks, definition of SLAs. All technical documentation will be provided in English or Romanian.
NFR 09.04 API documentation	The Consultant will prepare and deliver: • API integration guide • Integration samples at least in .NET and Java • Human and machine-readable description in a standard description language (e.g., WSDL or Swagger)
NFR 09.05 Training sessions	The Consultant will provide training sessions using developed e-learning modules for the following target groups: • System Administrators from EGA and STISC • Remote identification operators (2 groups of up to 10 people)
NFR 09.06 Training materials	Training documentation – curricula, training courses (manuals, video tutorials, quizzes, etc.) for administrators, services providers, and end-users shall developed in e-learning platform, called MLearn, which is based on Moodle. All training content/materials will be provided in Romanian.

5.10 Warranty and support

Requirement	Description
NFR 10.01 Warranty timeframe	The warranty period starts after final release and lasts for 12 months.
NFR 10.02 Warranty activities	During the warranty period the Consultant shall: • fix all defects reported by the Beneficiary, • solve all incidents reported by the Beneficiary according to the agreed SLAs. Note: The response and resolution time shall not exceed 4 hours for non-critical defects and 30 minutes in case of critical defects. The incidents shall be solved within 2 working days for non-critical incidents and within 4 working hours for critical incidents starting from escalation time. Hourly progress reports will be provided for critical items.

6 Annexes

6.1 Annex 1. References

The following materials were reviewed during the development of this document:

1) Remote ID Proofing — ENISA (europa.eu)[1]
2) Remote Identity Proofing - Attacks & Countermeasures — ENISA (europa.eu)[2]
3) eKYC & Identity Assurance WG | OpenID[3]
4) ETSI TR 119 460 - Electronic Signatures and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects.
5) ETSI TS 119 461 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
6) ISO/IEC 30107 - Biometric presentation attack detection

[1] https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing
[2] https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures
[3] https://openid.net/wg/ekyc-ida/

6.2 Annex 2. Relevant Legal Framework

The legal framework for the Reusable eKYC solution is established primarily by **Government Decision nr.74/2024 on government service for remote identification of persons**[4].

The following regulatory acts complement the legal framework for the Reusable eKYC solution:

1) Law nr.124/2022 on electronic identification and trust services[5]
2) Law nr.308/2017 on prevention and combating money laundering and terrorism financing[6]
3) Law nr.234/2021 on public services[7]
4) Law nr.1069/2000 on informatics[8]
5) Law nr.467/2003 on informatics and state informational resources[9]
6) Law nr.982/2000 on access to information[10]
7) Law nr.133/2011 on personal data protection[11]
8) Law nr.142/2018 on data exchange and interoperability[12]
9) Government Decision nr.128/2014 on Government single technological platform (MCloud)[13]
10) Government Decision nr.1090/2013 on the governmental electronic service of authentication and access control (MPass)[14]
11) Government Decision nr.405/2014 on the governmental electronic integrated service for digital signature (MSign)[15]
12) Government Decision nr.211/2014 on the interoperability platform (MConnect)[16]
13) Government Decision nr.708/2014 on the governmental electronic journaling service (MLog)[17]
14) Government Decision nr.376/2020 on the governmental notification service (MNotify)[18]

[4] https://www.legis.md/cautare/getResults?doc_id=142272&lang=ro
[5] https://www.legis.md/cautare/getResults?doc_id=131642&lang=ro
[6] https://www.legis.md/cautare/getResults?doc_id=136906&lang=ro
[7] https://www.legis.md/cautare/getResults?doc_id=129764&lang=ro
[8] https://www.legis.md/cautare/getResults?doc_id=132782&lang=ro
[9] https://www.legis.md/cautare/getResults?doc_id=132933&lang=ro
[10] https://www.legis.md/cautare/getResults?doc_id=136300&lang=ro
[11] https://www.legis.md/cautare/getResults?doc_id=136439&lang=ro
[12] https://www.legis.md/cautare/getResults?doc_id=129134&lang=ro
[13] https://www.legis.md/cautare/getResults?doc_id=136746&lang=ro
[14] https://www.legis.md/cautare/getResults?doc_id=128353&lang=ro
[15] https://www.legis.md/cautare/getResults?doc_id=128352&lang=ro
[16] https://www.legis.md/cautare/getResults?doc_id=128349&lang=ro
[17] https://www.legis.md/cautare/getResults?doc_id=128351&lang=ro
[18] https://www.legis.md/cautare/getResults?doc_id=128348&lang=ro

6.3 Annex 3. Digital ecosystem

MCloud

MCloud, the cloud government infrastructure, is a fully virtualized environment built on VMWare. It offers a cost-effective solution for hosting ICT solutions, eliminating the need for beneficiaries to invest in infrastructure such as data centers, servers, storage, networking devices, and security measures. This government-owned infrastructure, managed by the STISC, is renowned for its high level of security and advanced technology.

By leveraging MCloud, organizations can significantly reduce hardware maintenance costs as the responsibility is transferred to the technical administrator. Moreover, MCloud was specifically designed to enable multiple institutions to share common ICT solutions and applications, eliminating the need for individual server infrastructure and storage space.

The Government of the Republic of Moldova introduced the MCloud platform to optimize spending on ICT services and consolidate data centers under shared management. This initiative aims to reduce costs, enhance the quality of information systems, and improve their security for critical state operations.

Since its launch on February 14, 2013, the MCloud platform has been fully operational, and numerous public authorities have successfully migrated their digital content to this platform.

Starting from 2023, MCloud includes Kubernetes-as-a-Service, which is leveraged by EGA to host various information systems. EGA has developed standard templates for CI/CD and helm chart that will be leveraged by this solution.

MPass

MPass is a national service that enables authentication and access to digital public services. It offers various authentication methods, including mobile signature, digital certificate, and 2-step verification based on username, password, and OTP. EGA will soon add EVOSign as alternative innovative instrument for digital identity.

The MPass Server facilitates Single Sign-On authentication, granting users complete control over the authentication and authorization of their hosted user accounts.

It's important to note that the single-sign-on solution involves direct user interaction with the MPass website, which can also be integrated with native mobile apps.

Users with valid digital certificates can create accounts without requiring validation. The MPass server automatically extracts data from trusted digital certificates to create validated user accounts.

Upon successful authentication, MPass can be configured to return additional attributes from various state registries, such as the list of companies the authenticated person is Administrator of.

MPass is currently based on SAML v2 and EGA will provide the MPass Integration Guide, offering a comprehensive overview of the system architecture and detailing the process of system interaction for providing authentication services to third-party IT systems and software development teams. EGA has developed an integration library for .NET that will be leveraged by this solution.

MSign

MSign is the government's electronic signature service, offering a secure and versatile solution for using different types of electronic signatures in online interactions while ensuring the authenticity of the signatures.

Users can utilize three available tools through MSign: Mobile Signature, Electronic Identity Card, and Electronic Signature (STISC). Integrating the ICT solution with MSign allows for document signing within digital applications and certifying users' actions.

EGA will soon add EVOSign as alternative innovative instrument for applying digital signatures.

According to the Electronic Identification and Trust Services Law (No. 124 from 2022), electronic documents are equivalent to handwritten paper documents.

For MSign, EGA will provide an integration guide and has developed an integration library for .NET that will be leveraged by this solution.

MPay

MPay is governmental service for electronic payments, is an informational tool by which various services can be paid online. Although MPay is primarily targeting electronic services in the public sector, it can be successfully used for commercial services.

MPay enable payment services through multiple payment methods: credit cards, payment terminals, e-banking, and cash payments. For cash payments, people who do not have Internet access can contact the bank counters or post offices from Moldova for internet connection.

You can pay the consumed services with any legal instrument available on the market of Moldova. Through MPay you can even pay offline the services consumed, order which is made at the counter of public institutions. For this situation you can access the mpay.gov.md page, select the service and enter your order or service request number, after which you pay the same as you do at payment terminals.

MPay service is created by the Government through EGA, ITSEC, in partnership with the National Bank and the private banking sector. This service is in line with the National Bank policies that promote cashless transactions.

The MPay beneficiaries are citizens who pay for public services, business representatives who must charge fees for services rendered, and to pay for consumed services and even the public sector.

To integrate with MPay, EGA will provide an integration guide and has developed an integration library for .NET that will be leveraged by this solution.

MConnect

The Governmental Interoperability Platform - MConnect, serves to enhance the efficiency and quality of public service delivery by facilitating data exchange among authorities. This exchange occurs in real-time, eliminating the need for citizens and businesses to provide certificates, reports, and other documents.

The objectives of MConnect are as follows:

- Improve the efficiency and effectiveness of information systems used to deliver electronic public services.
- Optimize the utilization of public funds.
- Enhance citizen comfort and convenience.
- Enhance the security of information systems within local and central public administration.
- Promote resource reuse within information systems.
- Foster collaboration among public administration institutions.
- Enhance citizen comfort.

Data exchange within MConnect occurs through secure channels, utilizing standardized protocols and formats such as XML/SOAP, JSON/REST and HTTPS.

MConnect includes advanced mediation features, including advanced data transformations and data exchanged patterns, such as scatter-gather, parallel or sequential scenarios, etc.

EGA will guide you through integrating with MConnect to consume data using the MConnect Ambassador container, which significantly simplifies the integrations.

MLog

MLog is a centralized service designed to securely log and audit transactions or events within an information system. Its primary objective is to ensure the preservation of these transactions at specific times.

To facilitate the integration of information systems with MLog, EGA will provide the MLog Integration Guide. This guide describes the available technical interfaces that MLog provides for seamless interaction for synchronous logging and asynchronous querying of events. Additionally, EGA has an automatic asynchronous logging collection configured in its infrastructure for less critical events.

By following the guidelines outlined in the MLog Integration Guide, information systems can effectively connect with MLog, enabling the logging and auditing functionalities to operate smoothly and securely. EGA has developed an integration library for .NET that will be leveraged by this solution.

MNotify

MNotify is a software service specifically designed for sending notifications within the jurisdiction of public authorities and other public service institutions, using their respective information systems.

In this context, the term "Service" refers to an automated message generated by the institutions' information systems to inform users about changes in specific services or service delivery methods.

Through MNotify, users can receive timely notifications via email, SMS, instant messaging, or other communication channels, ensuring they stay informed about any relevant updates or reduced timeframes.

To facilitate the integration of information systems with MNotify, EGA will provide the MNotify Integration Guide. This guide outlines the necessary technical interfaces that information systems must expose to seamlessly integrate with MNotify, as well as the corresponding technical interfaces that MNotify provides for smooth communication. EGA has developed an integration library for .NET that will be leveraged by this solution.