Section 5. TERMS OF REFERENCE

Development and Implementation of the Forensic Case Management System (FCMS)

RFP No.: RfP21/02375

Project: Strengthening Efficiency and Access to Justice in Moldova

Country: Republic of Moldova

Section 5. Terms of Reference

Contents

1. Scope of the Document

This document describes the Technical Requirements which includes the functional and non-functional technical requirements for the Forensic Expertise Cases' Management ICT solution (FCMS), to be implemented within the UNDP "Strengthening Efficiency and Access to Justice in Moldova" Project (A2J Project).

This Technical Requirements document provides the classification of FCMS functionalities for the users from the national forensic institutions[1] and other external actors as well.

The functionalities mentioned above are presented both graphically through use case diagrams (UML Use Cases) and through narrative descriptions.

At the same time, the document addresses issues related to the ICT infrastructure and interoperability with other external ICT systems / tools. In this regard, the document describes some aspects of the governmental ICT infrastructure as well as of certain governmental platform services, which can be used to implement the FCMS.

The document also contains recommendations on the project implementation approach, the preliminary implementation plan and the proposed project governance model.

2. Background

The UNDP project "Strengthening Efficiency and Access to Justice in Moldova" (A2J) is a multi-year institutional development project designed to contribute to an increased efficiency of justice services and to improved access to justice of men and women in Moldova, in particular from vulnerable and marginalized groups, through enhanced capacities of forensic institutions to provide qualitative justice services, strengthened capacities of the justice sector actors in the selected pilot areas to provide coordinated response to men's and women's justice needs and strengthened civil society able to claim the respect of rights and engage in a constructive dialogue with the justice chain actors. Project interventions will offer and encourage equal opportunity for the participation of men and women.

Although important efforts have been deployed at national level during the last years to advance the efficiency, transparency, fairness and accessibility of the justice sector, improvement is further required to ensure coherent coordination among law enforcement, security and justice institutions for effective administration of justice, so that men and women, particularly from marginalized or minority groups, are able to claim their rights and access justice effectively.

The system of forensic institutions[2] is an integral part of the justice system. The expert opinions provided by these institutions are critical for the objective and evidence-based delivery of justice. The quality and accuracy of forensic investigations and examinations have an extensive impact on the quality of justice and affect the overall perception of users about the justice system.

Despite the importance of forensic examination for the act of justice, the institutional system of judicial expertise has not enjoyed the same attention, assistance and support in its modernization and e-transformation efforts, as in the case of other actors of the justice sector.

For example, the judicial system has enjoyed consistent support for the development, implementation and sustainability of the PIGD information system, and the Prosecutor's Office, with the support of development partners, has initiated and continues to implement the 'e-File' information system.

Although significant efforts have been made nationally in the recent years to promote the efficiency,

[1] Within the scope of the A2J Project technical assistance is provided to the following three institutions the National Centre for Judicial Expertise (NCJE), Forensic Centre of the General Police Inspectorate (Police Forensic Centre) and Centre for Legal Medicine (CLM).

2 The system of judicial expertise institutions includes public institutions of judicial expertise and private forensic experts' bureaus. In line with the art.65 para.(2) Law no. 68/2016 on the Judicial Expertise and the Status of Judicial Expert, the system of public institutions of judicial expertise includes the specialized institutions of the Ministry of Justice and the Ministry of Health, Labor and Social Protection, the operative technical-forensic subdivisions or judicial expertise of the Ministry of Internal Affairs and the National Anticorruption Center. The state can also create other public institutions of judicial expertise.

transparency, fairness and accessibility of the justice sector, further improvement is required to provide consistent coordination between institutions for a more efficient management of the justice sector, so that both men and women, especially those of vulnerable groups, are able to claim their rights and access justice equally and effectively.

Thus, the UNDP Project 'Strengthening efficiency and access to justice in Moldova' (A2J Project), provides support for institutional development, as it is designed to support achieving a higher efficiency of services the justice sector and to increase access to justice for everyone.

3. Acronyms and Definitions

List of acronyms used in this document:

#	Acronym	Explanation
1	API	Application Programming Interface
2	AIS	Automated Information System
3	CLM	Centre for Legal Medicine
4	DB	Database
5	DBMS	Database Management System
6	FCMS	Forensic Case Management System
7	GB	Gigabyte
8	GUI	Graphical User Interface
9	HTTPS	HyperText Transfer Protocol Secured
10	ICMP	Integrated Case Management Platform used in by the courts in Moldova
11	ICT	Information and Communication Technologies
12	IS	Information System
13	ITCSS	IT and Cyber Security Service
14	MoJ	Ministry of Justice
15	NCJE	National Centre for Judicial Expertise,
16	OS	Operation System
17	RAM	Random Access Memory
18	RM	Republic of Moldova
19	RPO	Recovery Point Objective
20	RTO	Recovery Time Objective
21	SAML	Security Assertion Markup Language
22	SDS	System Design Specification
23	SOA	Service-Oriented Architecture
24	SOAP	Simple Object Access Protocol
25	SRS	System Requirements Specification
26	SSO	Single Sign-On

#	Acronym	Explanation
27	POLICE FORENSIC CENTRE	Forensic and Judicial Expertise Centre under the General Police Inspectorate
28	UML	Unified Modeling Language
29	UNDP	United Nations Development Programme
30	WSDL	Web Services Description Language
31	XML	eXtensible Markup Language

List of definitions used in this document

#	Definition	Explanation
1	Actor	Role of a user or other system that interacts with the information system.
2	Component	Any subsystem, module or subset of the System identified as an integral part of the System.
3	Database	Data collection organized according to a conceptual and well-defined structure, which describes the basic characteristics and the relationship between entities.
4	Forensic Report	Forensic report, non-forensic report, technical and scientific fact-finding report, forensic medical fact-finding report.
5	Logging	A function for recording information about events that take place in a system. In information systems, event records include details about the date, time, user and taken action.
6	Request (application)	An order to conduct a judicial expertise (an order of a criminal investigation body or a court order, authorizing performance of the judicial expertise or, as the case may be, a request for the conduct of forensic examination submitted by the parties on their own initiative and on their own account under the under the terms set out in the Civil Procedure Code, Criminal Procedure Code and Contravention Code, a written request of a natural or legal person regarding the performance of a non-judicial expertise).
6	Requester (Applicant)	Orderer of forensic examination (investigation body, court or another involved party to proceedings conducted under the terms set out in the Civil Procedure Code, Criminal Procedure Code and Contravention Code law of civil, criminal or contravention procedure, which has the right to order or request independently the conduct of a forensic judicial expertise; a natural or legal person who

#	Definition	Explanation
		usually carries out a non- judicial expertise)..
7	Workflow	A series of tasks to produce a desired outcome, usually involving multiple participants and several stages in an organization.
8	Informatic System	Set of programs and equipment that ensure automated data processing.
9	Information System	A system for processing of information, together with associated organizational resources, such as human and technical resources, that provide and distribute data/information.
10	System	Forensic Case Management System (FCMS)

4. General Description of the Project

4.1. Scope

The main purpose of the Forensic Case Management System (FCMS) is to contribute to the improvement of the processes management and keeping of records of data, information and documents related to the field of judicial expertise[3] , as well as to ensure the custody of evidence – the objects that are subject to judicial expertise , by providing a modern integrated management tool, bringing together in a single information space all the data and processes in which the staff of the national forensic institutions is involved, as well as the employees of other public authorities/institutions within the justice chain of the Republic of Moldova, which according to national legislation have the role of demanders of judicial expertise .

4.2. Objectives

The implementation of the FCMS aims to achieve the following objectives:

- Create an information resource for the national forensic institutions in order to produce, store, systematize and update the information processed by these (e.g. requests, forensic cases and related documents, judicial expertise reports, etc.) and to ensure an adequate level of data protection;
- Streamline the work of the personnel of the national forensic institutions by replacing the method of collecting and recording information on paper with the electronic storage and processing of relevant data in the context of their daily activity related to the judicial expertise;
- Ensure the chain of custody of objects subject to judicial expertise;
- Ensure the quality and accuracy of the information handled in the course of judicial expertise;
- Ensure unique identification, management and custody of documents, records, case-files and/or reports part of the processes related to forensic examination, as well as other documents later identified in coordination with the national forensic institutions;
- Remove the burden of manually filling of various registers and reports on paper. As such these shall be generated from the FCMS based on the primary data entered into the system;
- Centralize all data and information related to forensic cases in a single database and provide access to both aggregated and detailed information of different forms and formats;
- Ensure data protection and other aspects of information security related to forensic examination;
- Reduce the time required to collect the necessary data and time to prepare and consolidate integrated reports by using a modern reporting tool such as BI (Business Intelligence). This will ensure that statistical and analytical reports, both predefined and custom ad-hoc, are generated.
- Ensure the connection of the requesters of judicial expertise to an unique virtual workspace.

4.3. Limitations of the scope of the Project

The following limits are pre-set for the FCMS development and implementation project taking into account that the System will be hosted in MCloud government infrastructure:

- Upgrade or re-engineering of other software solutions that the FCMS may come into contact with

[3] For the scope of this ToR the term “judicial expertise” is used as a close equivalent of “forensic activity” or “forensic/expert investigation”. Thus, the word “expertise” refers not only to the body of certain specialized knowledge but also to the process of conducting forensic/expert investigations or examinations. This is made in order to remain close to the original term of “expertiza judiciara” used in Moldovan law. It should not be confused with judicial knowledge, judges or other professionals’ experience or expertise, etc.

through electronic data exchange are not part of the scope of this project;

- Purchase of hardware equipment (e.g. servers, storages, networking devices, etc.) does not fall within the scope of the project described in this document;
- Activities regarding the data-center arrangement are out of scope;
- Purchase and installation of software at the client level (e.g. Windows OS, MS Office packages) are out of scope of this project;
- Purchase of electronic signatures in the form of sticks or mobile signatures for end-users, is out of scope of this assignment;
- Training services on the use of the FCMS are to be provided primarily to users from the national forensic institutions and other public authorities, as appropriate. For the 'requester' user role, the user guide and video tutorials will be made available, that must be accessible through the web pages of the targeted institutions;
- The mass training of the Requesters[4] on how to use the computer and the Requester's Virtual Cabinet is not included in the project activities.

4.4. Key Stakeholders

In line with the scope of the A2J Project and the objectives of the FCMS development and implementation project, the preliminary list of the key stakeholders for this project is listed bellow:

National Centre for Judicial Expertise (NCJE)

National Centre for Judicial Expertise is a state institution specializing in the field of conducting judicial expertise and provision of technical-scientific findings. NCJE acts as well as a coordinating institution of the theory and practice of judicial expertise, develops methods and observes their application in practice, contributing thereby to justice in Republic of Moldova. NCJE is one of the beneficiaries of the FCMS.

Main tasks of NCJE are:

- Conducting judicial expertise and provision of technical-scientific findings;
- Generalization and analysis of the practice of conducting expertise and technical-scientific findings, developing and implementing measures to improve forensic and other types of research;
- Judicial training and retraining of experts of the centre;
- Studying the scientific achievements of other countries in the field of judicial expertise, collaboration with similar institutions, scientific and educational organizations in order to improve practice expertise and extend its possibilities.

Forensic and Judicial Expertise Centre under the General Police Inspectorate (Police Forensic Centre)

Forensic and Judicial Expertise Centre under the General Police Inspectorate under the Ministry of Interna Affairs supports criminal investigation bodies such as Prosecution, Police and Customs through technical and

[4] For the scope of the ToR, Requester shall include as specified in LAW No. 68 of 14.04.2016 on Judicial Expertise and Judicial Expert Status, the Judicial Expertise Authorising Person – a criminal investigation body, court or other party in proceedings pending according to the legislation on civil criminal, or contravention procedure (hereinafter referred to as procedural legislation), entitled to order or request independently a judicial expertise to be conducted.

forensic discovery and investigation. Police Forensic Centre is one of the beneficiaries of the FCMS.

Main functions of the Police Forensic Centre are:

- Provision of judicial and technical-scientific findings;
- Analyze and summarize the practice of judicial expertise , technical-scientific findings, take measures aimed at detecting and investigating crimes by conducting judicial expertise and technical scientific findings;
- Implement modern and efficient examination procedures for drawing up reasoned conclusions in evaluating the circumstances and causes of crime;
- Organizes seminars theoretical and practical exchanges and trainings with participation of employees from Police subordinated subdivisions and other law enforcement agencies;
- Carry out training and subsequent award in the established qualification of judicial expert and tasks certification and qualification degree of judicial experts.

Centre of Legal Medicine (CML)

CML is a public institution with the mission to contribute to justice by conducting judicial expertise and forensic findings. CLM is one of the beneficiaries of the FCMS.

Main functions of the CLM are:

- Participation in development of strategies in forensic medicine and ensuring their implementation;
- Contribution to the elaboration of normative acts within judicial expertise domain;
- Ensuring the development of normative acts on forensic examination;
- Ensuring common forensic practices across the Republic of Moldova.

Ministry of Justice of the Republic of Moldova (MJ)

Ministry of Justice of the Republic of Moldova represents the owner of the Forensic Case Managemet System (FCMS).

United Nations Development Programme (UNDP) in the Republic of Moldova

UNDP A2J Project represents the project management entity for the implementation of the FCMS project. Currently, the ICT technical expertise and procedural advisory services to modernize the field of judicial expertise are provided by the UNDP's experts.

Electronic Governance Agency (eGA)

Electronic Governance Agency is a public institution subordinated directly to the State Chancellery (Government), which aims to improve governance through the intensive use of information technologies. eGA has a systemic approach to modernize public services and bring governance closer to the business and citizens of the Republic of Moldova.

eGA pursues the following objectives:

- Modernization of public services by digitizing and retaining them;
- Streamlining governance through the exchange of data between authorities and institutions providing public services;
- Diversification of access channels to public services;
- Ensuring information security.
- EGA has a very important role in the process of coordinating and implementing any ICT solutions designed for the state bodies of Moldova.

Information Technology and Cyber Security Service (ITCSS, ro: STISC)

For the scope of the FCMS implementation the ITCSS will have the role of Technical Administrator of the FCMS IS. ITCSS is currently the entity responsible for the management and operation of the cloud government

infrastructure – 'MCloud'. As the operator of the governmental cloud infrastructure and electronic services, ITCSS has the mission to ensure the administration, maintenance and development of information technology infrastructure, telecommunications system of public administration authorities, as part of the special communications network and state information systems, infrastructure management of the electronic signature, as well as the implementation of state policy in the field of cyber security.

Among other stakeholders for may be mentioned:

- General Prosecutor Office;
- Courts of Justice;
- National Anticorruption Center – may become in the future another beneficiary of the FCMS, as the institution also provides judicial expertise
- Moldovan Border Police – may become in the future another beneficiary of the FCMS, as the institution also provides judicial expertise ;
- Private bureaus of judicial expertise ;
- Citizens;
- Economic operators;

The list of the stakeholder might be extended during the detailed Analysis and Design Phase of the Project.

5. Relevant Legal Framework

The following regulatory acts were consulted during the analysis and description of the FCMS architecture:

- Law No. 68 of 14.04.2016 on judicial expertise and judicial expert status;
- Law No. 982/2000 on the access to information;
- Law No. 91/2014 on the electronic signature and the electronic document;
- Law No. 142/2018 on data exchange and interoperability;
- Law No. 133/2011 on personal data protection;
- Law No. 467/2003 on computerization and state information resources;
- Law No. 71/2007 on registers;
- Government Decision No. 546/2011 on the approval of the Regulation on the provision of services of the Telecommunications System of public administration authorities and on amendments to some Government decisions;
- Government Decision No. 840/2004 on the creation of the Telecommunications System of public administration authorities;
- Government Decision No. 128/2014 on the common government technology platform (MCloud);
- Government Decision No. 211/2019 on the interoperability platform (MConnect);
- Government Decision No. 1090 of 31.12.2013 on the government electronic service of authentication and access control (MPass);
- Government Decision No. 329 of 28.05.2012 on the Government Electronic Payments Service (MPay);
- Government Decision No. 405/2014 on the integrated government electronic service of electronic signature (MSign);
- Government Decision No. 708/2014 on the governmental electronic journalism service (MLog);
- Government Decision No. 376/2020 for the approval of the Concept of the government notification service (Mnotify) and of the Regulation on the functioning and use of the governmental electronic notification service (MNotify);
- Government Decision No. 710 of 20.09.2011 on the approval of the Strategic Programme for Technological Modernization of the Government (e-Transformation);
- Other normative acts and internal procedures related to each involved forensic institution will be provided to the selected the Contractor.

6. Risks

Risk	Impact	Mitigation strategy
Staff rotation could affect the operation of the System. Between the first training sessions and launching of the new System, some employees may leave being replaced, which will require additional training.	Medium	It is proposed to carry out ToT (Training of Trainers) type of trainings, so that all the necessary knowledge about new System can be facilitated by certain key employees selected by the beneficiaries.
Requesters could still opt for old traditional methods of submitting of paper documents. At least for the first period such a reaction is expected.	Low	It is proposed to organize information campaigns, especially among public authorities about the availability of a new e-service, with appropriate explanations that provide clarity about the interaction with Forensic institutions through the new System for FCMS, about the availability of the "virtual cabinet" which is legal and equivalent to the classic approach, but offers more comfort and efficiency to those who have to submit requests for judicial expertise .
Different level of knowledge of users in terms of using computers and information technologies	Medium	FCMS shall be a web-based software solution with a user-friendly graphical user interface in Romanian language, so its use will not be more complicated than browsing a website.
Different level of ICT infrastructure at user level (PCs, operating systems, etc.).	Medium	Since the FCMS IS shall be a web-based solution, it will not require the installation of certain programs or third-party applications at the user level and will not depend on the technical requirements of the user's computer. All the user will need is a simple web browser, such as Mozilla Firefox, Google Chrome or Microsoft Edge.
Inadequate implementation of the project, by providing deliverables from the supplier that would not meet the technical requirements or of poor quality	High	It is recommended to involve a technical supervisor of the project – an experienced specialist in implementation of ICT projects. It can be designated directly by the MJ or proposed by the UNDP A2J Project. He/she shall be responsible for verifying all deliverables from a technical and contractual point of view. At the same time, he/she shall coordinate all the testing sessions of the modules and the System as a whole in order to be convinced that what the software product is delivered and corresponds to the requirements of the specifications and the expectations of the Beneficiary.
Post-implementation abandonment of the project due to certain non-conformities detected too late	Medium	The contract on the implementation of the FCMS necessarily includes the maintenance and support warranty period which shall be provided by the contractor (supplier of the ICT solution). This is foreseen for one year and may be subsequently extended by MJ, if so will be agreed by parties. During this period, any detected non-conformity must be corrected by the supplier on behalf of the existing contract, without requesting additional resources.

7. Requirements' Traceability

To ensure traceability of requirements, the document follows naming conventions in order to identify and track all technical specifications set out for development and implementation of the System.

As there will be more documents compiled during development of the FCMS, the reader can easily go back and forth through the list of specifications using the provided reference numbers.

Each reference number is preceded by an abbreviation consisting of several letters, which classifies the requirement. The prefix is followed by a sequential number corresponding to the business process step. For example, FRQ007 and FRQ008 are reference numbers for two functional requirements. NFRQ is reference for non-functional requirement.

In this naming convention, letters in the prefix denote the following:

- FRQ – Functional requirement;
- NFRQ – Non-functional requirement;

Each functional or non-functional technical requirement could have the following marks:

- (M) = Mandatory = "The System must ...";
- (HD) = Highly Desirable = "The System shall ..."; and
- (D) = Desirable = "The System may ...";

Where:

- MUST – means that the requirement is defined is an absolute have requirement;
- MUST NOT – means that the numbered requirement is defined is an absolute prohibition.
- SHOULD – means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

The described functionalities have the accompanying use-case diagram, which elaborates the requirements in a more detail way and presents the business context in which the System functionality is used. The detailed design that will be provided by the selected Supplier will have the detailed description of the functionalities.

8. Conceptual Architecture

General Aspects

FCMS has been conceptually divided into functional components, which encompass the possibilities of the System that shall be made available to the users.

Please note that the names of the components below are conventionally.

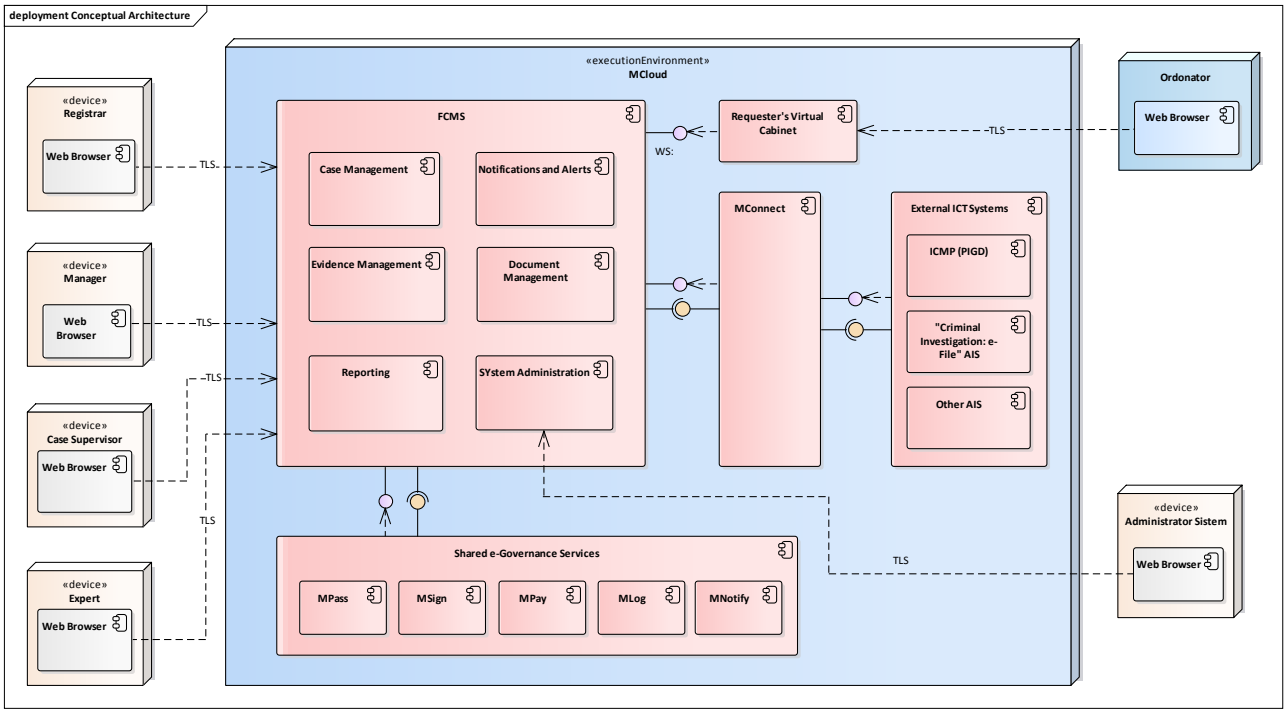


Figure 1. Conceptual Architecture

It should also be noted that any business entity in the System, such as document, report, etc. will be assigned a unique identification number in order to ensure the traceability and avoid it being confused with another entity.

From the architectural point of view FCMS shall be designed as a modular, configurable web-based software solution that encompasses several functional components. Each system component represents a group of functionalities and may contain a set of use cases that define how an actor can interact with the System (FCMS).

In other words, FCMS has been conceptually divided into functional components, which include the possibilities of the System that shall be made available to the users.

The FCMS system components listed below are preliminary and they must be detailed at the stage of Detailed Analysis and Design.

The '**Case Management**' system component will realize in the System the so-called Case Management concept. Thus, the System shall cover at least the following aspects:

- Registration of requests/applications for judicial expertise that are submitted by the requester;
- Generation of the unique identification code (unique ID) of each request and uploading into the System, including all appropriate metadata;
- Creation of the electronic case based on the received request, generation and assignment of the unique ID, completion with relevant metadata and inclusion of other documents in the case;
- Ensuring the custody of the case and tracking its evolution throughout the entire lifecycle, through the statuses set automatically by the System, from its initiation till its completion. All names of statuses presented in the flows are conventional and must be exactly established during the detailed analysis and

design phase of the System;
- Ensuring the appropriate access to the information from the registered forensic cases according to the hierarchical model of users and taking into account the stage of the flow in which the case is located;
- Implementation of a mechanism for distribution and assigning of cases among subdivisions and users from the involved forensic institutions, including the cases of complex judicial expertise ;
- Implementation of the decision-making mechanism in the System through validation/approval features and including applying of electronic signature.

The 'Evidence Management' system component will be dedicated to activities related to keeping of records about the objects that are subject to judicial expertise (*things, substances, traces, documents, facts, phenomena, circumstances, human body and psyche may constitute the subject-matter of judicial expert investigation and shall be examined to uncover the truth*).

The keeping of records and management of evidence will be carried out by methods of strict record keeping by using barcodes, and shall include at least the following possibilities:

- Receiving the objects subject to forensic examination from the requesters and their primary registration in the System by applying the barcode and associating them with the unique ID of the forensic case;
- Automation of reception and transmission of evidences between subdivisions and users within the forensic institutions;
- Ensure the strict record keeping and the chain of custody of the objects subject to forensic examination;
- Connection to the System of the necessary equipment for keeping records about the objects subject to forensic examination, such as thermal barcode printers and barcode scanners.

The '**Document Management**" system component shall implement document management elements, which will enable processing of incoming and outgoing documents in the forensic institutions.

Through this component, a unique identification number (ID) will be generated and assigned for the incoming documents, which will be loaded into the System and linked to a forensic case, if so needed;

Some outgoing documents could be generated based on a predefined template and subsequently filled in by the user and electronically signed, if so required. These can be subsequently submitted either electronically or printed on paper.

Filling in different paper-based incoming/outgoing registers would no longer be a necessity, as they can be generated automatically from the System.

The '**Reporting**" system component will be dedicated to the generation of both predefined statistical and analytical reports, as well as those generated on ad-hoc basis. Thus, the FCMS will automate the reporting process within the forensic institutions and will provide at least the following features:

- The data reflected in the reports shall be collected and processed during users' daily activities;
- The System shall enable defining the relevant parameters for generation of reports, for example: type of forensic examination, case status, requester, etc.;
- The FCMS shall enable printing of reports and their export in formats such as HTML, MS Excel, MS Word, XML and PDF;
- The FCMS shall also provide support for subscription to reports for some of the users from forensic institutions, by receiving generated reports by e-mail at pre-set time intervals, configured based on the criteria defined by the subscribed user;
- The FCMS shall provide various reporting formats, such as tabular format or graphical representation. The user must be able to select the format of each report to be generated;
- The FCMS shall ensure that new types of reports can be added in a simple and intuitive way.

Thus, the FCMS shall offer the possibility to save the configuration of the criteria according to which a report is

generated, so that users (Managers, Case Supervisors and Experts) can later return to a certain report template.

The FCMS shall also contain a predefined series of reports-registers, which will be generated by the System, such as:

- Registry of incoming/outgoing documents;
- Registry of requests for forensic examination;
- Registry of correspondence within forensic processes;
- Registries per institution and internal departmental registers;

Other predefined reports – to be established by the co-beneficiary forensic institutions during the FCMS Analysis and Design phase period.

- The FCMS shall offer the option of drill-down in reports, from a general level to a more detailed level of representation;
- The FCMS will enable searching for generated reports and will implement the web-based reporting interface. Report templates will be managed by the System Administrator and will include a tool (web user interface) for report modelling;
- The FCMS will enable users to set filtering and sorting criteria when running reports.

The '**Notifications & Alerts**" system component will notify accordingly System's actors depending on their role and event.

For example, Experts must be notified by the System when a new forensic case is assigned to them. The Requester may be notified of the completion of the forensic examination and the availability of the final forensic report.

Any user in the System could be alerted if a certain deadline set for one of its tasks is about to expire.

The notification/alerting means and mechanisms are to be established during the Analysis and Design Phase of the Project. These can be, for example: e-mails, SMSs or notifications via the user's dashboard. The 'Requester's Virtual Cabinet' component is intended to provide a dedicated virtual workspace in the FCMS for the requesters. This component is seen as a public web portal connected to the FCMS platform.

The requesters must be able to use the governmental authentication service MPass for authentication where they will have access to at least the following possibilities:

- Access to the user's dashboard, where he/she can quickly view the information relevant to his/her activity in contact with the forensic institutions;
- Receiving of notifications/alerts on the status of their submitted requests. The FCMS shall be able to create e-mail messages according to the pre-set templates and subsequently to send them to the beneficiaries;
- Tracking the status of the submitted requests/ongoing forensic cases;
- Viewing the history of submitted and processed requests;
- Access to forensic, non-forensic, fact-finding reports, in electronic format and signed with digital signature;
- Features of communication with forensic institutions, if applicable in a forensic process.

The 'System Administration' component shall address at least the following:

- The FCMS shall provide features for managing the organizational structure of each involved forensic institution. Thus, the System Administrator must have the possibility to add, modify or deactivate any institution's subdivision.
- The FCMS shall not enable deactivation of the subdivision, if it is an active one, i.e. it is involved in processes, there are active forensic cases and related documents, activities, etc.
- The FCMS shall provide the System Administrator with the user management feature. He/she must

be able to attach roles to each user and necessarily indicate the subdivision where he/she works.

- The FCMS shall provide the System Administrator with role management features. In this context, the System Administrator must be able to set the necessary permissions: the level of access to data and the level of access to features.
- The FCMS shall provide the System Administrator with features to configure the notifications/alerting mechanism. He/she will be able to configure alerts for at least the following events:
    - Receipt of a new forensic request/application;
    - Changing the status of a case;
    - Expiration of a deadline;
    - Emergence of new tasks, which require the user's attention;
    - Other events to be determined during the Analysis and Design phase of the project.

  When configuring notifications/alerts, the FCMS will enable the System Administrator to indicate:
    - The event of notification;
    - Who is the user to receive the notification;
    - Content (text) of the notification;
    - The time of notification;
    - Frequency of notification and other relevant parameters.

9. Interoperability

The FCMS interoperability is a feature of communication with other external software solutions.

To support the entire set of work processes related to forensic examination, and to provide relevant information throughout the whole judicial chain of the Republic of Moldova, data exchange mechanisms with other information systems relevant to the concerned field shall be implemented in the FCMS.

Given the current legal framework and the available government ICT infrastructure, it is currently recommended that the data exchange be carried out through the MConnect interoperability platform. To ensure this aspect, the FCMS must provide interfaces based on open standards.

In the context of this document, it is proposed that the FCMS be interconnected with the following electronic services and ICT systems:

- Government authentication and authorization service 'MPass'. For more details, please see ANNEX 14.1 Governmental ICT Infrastructure.
- Government electronic signature service 'MSign'. For more details, For more details, please see ANNEX 14.1 Governmental ICT Infrastructure.
- Government electronic payment service 'MPay'. For more details, For more details, please see ANNEX 14.1 Governmental ICT Infrastructure.
- Logging service 'MLog'. For more details, For more details, please see ANNEX 14.1 Governmental ICT Infrastructure.
- Government notification service 'MNotify'. For more details, please see ANNEX 14.1 Governmental ICT Infrastructure.
- The Integrated Case Management Programme 'ICMP' (PIGD) implemented in courts;
- The automated information system 'Criminal investigation: e-File System", of the General Prosecutor's Office;
- State Population Registry for identification, taking over and verification of information about individuals in the Republic of Moldova;
- State Register of Legal Entities – for identification, processing and verification of information about legal entities in the Republic of Moldova;
- Other external information systems that can be identified later at the stage of detailed analysis and design, development of the technical solution.

It is required that FCMS to provide interfaces that can interact with external ICT solutions in real time. The System's interfaces shall enable interacting with external ICT applications and e-services (message-based communication).

The FCMS software solution shall provide standard interfaces to access all System key-functions (e.g. document generation, transactions, access to information about any entities stored in the System). The interfaces must enable the management of business entities by applying all relevant business-logics rules.

All aspects related to the interoperability of the FCMS shall be documented accordingly (e.g. by using the WSDL model – standard web services description language).

10. FUNCTIONAL REQUIREMENTS OF THE SYSTEM

Each user's interaction can be specified using Use Case diagrams and narrative descriptions, which together describe how the System as an entity interacts with a user.

The Use Case Model is a catalogue of the FCMS functionalities described in UML - Use Cases. Each use case represents a single repeatable interaction that a user or an "actor" can perform when using the System.

A use case typically includes one or more "scenarios" that describe the interactions between the Actor and the System and document the results and exceptions that arise from the user's perspective.

Use cases may include other use sub-cases as part of a broader interaction model and may be extended to other use cases to address exceptions.

The use cases diagrams included in this document are indicative and shall be detailed during the Analysis and Design Phase of the project.

10.1. System's Actors

Actors are users of the modelled System (FCMS). Each actor shall have a well-defined role and, in the context of this role, will interact with the System and other actors through the provided features.

Any System (non-human actor), such as another software or DB, can be also an actor.

In the context of this document several FCMS' actors have been identified.

Some of the roles can be played by one or more persons depending on the circumstances i.e. structure and organization of the institution/subdivision. This aspect may vary from one institution to another.

The following are the main actors of the FCMS. The contractor together with the beneficiary forensic institution may adjust and detail the list of the actors during the Analysis and Design Phase of the project.

#	Actor	Explanation
1	Registrar	The role of Registrar in the System is played by the user with registration duties. This role is usually fulfilled by an employee of the secretariat subdivision of the forensic institution. In the case of territorial subdivisions of the CLM, this role can be performed by the nurse, who is responsible for recording the forensic requests for forensic examination. The Registrar will be responsible in the FCMS for receiving the requests, uploading them in the System and filling the electronic form of the request (application). Likewise, the Registrar shall have access to features related to the processing of incoming and outgoing documents, as the FCMS will also contain Document Management elements.
2	Requester	The Requester represents the *Expertise Requesters* [5]– those who have the right to request conducing of judicial expertise, as listed in the Law no. 68/2016, i.e. the criminal prosecution body, the court or another participant in the

5

#	Actor	Explanation
		process carried out according to the legislation regulating the civil, criminal or contravention proceedings, which has the right to direct or request independently conducting a judicial expertise (examination). Natural or legal persons requesting a forensic examination are also considered requester in the context of FCMS. The requester may or may not interact with the System. He/she can submit the request and pick up the forensic examination report according to the existing scenario – on paper; or can interact with the FCMS through the so-called "Requester's Virtual Cabinet", where he/she can track the status of submitted requests, as well as access other information relevant to forensic examination, including the final forensic examination report.
3	Manager	The role of the Manager may be performed by the director of the institution or the deputy director. At the same time, the features of this role can be delegated, for example, to a manager of the territorial subdivision. This configuration remains at the discretion of each forensic institution and is related to its Internal organization and distribution of roles and responsibilities. The manager can have read-only access to the data of any forensic case within his/her institution. He/she has access to features of making decisions and distributing cases to other relevant subdivisions, as well as power to sign cover letters for forensic reports. The manager may run statistical and analytical reports that may contain data at the level of any forensic case registered within the institution where he/she works.
4	Case Supervisor	The Case Supervisor is usually represented by the head of a subdivision/section or laboratory. He/she may have access to the information and data of the cases from his/her subdivision and may not have access to the cases from other subdivisions even if they belong to the same institution. The Case Supervisor has access to the features of completing the relevant sections of the electronic forms of the requests for forensic examination and for distribution of cases to forensic experts. He/she may also examine, return to the expert for completion or accept the forensic report. The Case Supervisor may run statistical and analytical reports that may contain only data from the cases distributed within his/her subdivision.
5	Expert (Judicial Expert)	The role of Expert is represented by the responsible forensic expert for carrying out the judicial expertise. He/she has

#	Actor	Explanation
		access in the System to the cases that have been distributed/assigned to him/her, can complete the relevant electronic files, generate and attach documents to the forensic case. The expert is responsible for generating and completing the forensic report, as well as for including all relevant annexes. This user can edit the report as long as it is not signed yet. The expert shall apply the qualified advanced electronic signature to the forensic report.
6	Depositary	The depositary is a virtual and conventional role in the System, which is responsible for the registration and keeping records of the operations on reception/transmission of the evidences (objects) of forensic examination, as well as for their primary registration into the System. These features may be combined by other user roles. In many cases, the responsibility for the primary registration of the evidence of forensic examination will fall on an employee of the subdivision or the person responsible for the secretary activity in the institution – the Registrar. The configuration of the rights of access to such features remains at the discretion of each forensic institution, according to its specifics.
7	System Administrator	Technical person, specialist in the field of information and communication technologies – responsible for the technical administration and configuration of the FCMS.

10.2. General Requirements to the FCMS Solution

Requirement's Identifier	Type	Explanation
FRQ001	M	The FCMS must offer the possibility of creating the organization structures (subdivisions/departments) for at least the following national forensic institutions: • National Center for Judicial expertise (NCFE); • Technical-Criminalistic Center of Judicial expertise (Police Forensic Centre); • Center of Forensic Medicine (CLM);
FRQ002	M	The FCMS (System) must allow the registration and

Requirement's Identifier	Type	Explanation
		management of cases during their entire lifecycle.
FRQ003	M	The FCMS must generate unique Case ID numbers in predefined configurable format depending on each forensic institution. The case number will be kept unique during the completely case's lifecycle.
FRQ004	M	The FCMS must provide web-forms for ensuring capture of main case metadata. These forms will include some mandatory and optional data fields, which will completed by the users, according to each stage during the workflow.
FRQ005	M	Each FCMS authorized user will have a dashboard to be notified of important process events, to quickly access details and to view the upcoming activities. Specifically, on the user dashboard, the following categories of information must be listed (available depending on the roles and rights, available to authorized users of the FCMS): • Active Cases • Scheduled tasks for the current period; • Planned tasks for the upcoming period; • Notifications of tasks which the user is required to perform; • Notifications concerning the progress of case(s) workflows related to the user; • Deadline notifications of completion of the tasks assigned to the user; • Notifications concerning the progress of the case(s) materials that are awaiting approval by the user; • Quick access by the user to the most recently accessed cases/documents;
FRQ006	M	The FCMS must display on the user's dashboard only relevant events, data and functionalities that are available as per the user's rights and role.
FRQ007	M	The FCMS users from the forensic institutions shall have dedicated workspaces, with navigation capabilities in relation to specific informational content. The workspace shall allow users to get to the detailed information available per specific content available in the workspace, which will allow the users to better organize their work and will provide the necessary information at their disposal. The FCMS will allow users to send files via their workspace.

Requirement's Identifier	Type	Explanation
FRQ008	M	The FCMS will provide for each case a dedicated electronic folder divided into several compartments (folders) dedicated to different stages of the main workflow e.g.: • Receiving and registration of the request/application for judicial expertise ; • Distribution of the case; • Preparation of the judicial expertise report; • Etc. The exact compartments shall be identified and described in details during the Analysis and Design Phase of the project together with the national forensic institutions.
FRQ009	M	The System must allow registration, editing and listing information about the Requester (Applicant).
FRQ010	M	The System shall allow uploading of files with allowed extensions only. The list of allowed types of files shall be configurable. The FCMS will ensure multiple files upload (bulk upload).
FRQ011	M	The FCMS shall generate documents (in .PDF format) based on predefined document templates and data from the database.
FRQ012	M	The FCMS must allow uploading of files and assigning them to a specific case.
FRQ013	M	All documents generated by FCMS must be stored into System together with uploaded files. The System will provide access to these documents only to the users that have appropriate permissions. Each user will have access to the documents related only to the case(s) that are assigned to this user. Under no circumstances an user may have access to the files, information and data, if this user is not involved in the respective judicial expertise case.
FRQ014	M	The System must ensure versioning functionality for all uploaded documents, as well as for the documents generated by the System. The FCMS will store and provide access to all versions of the files as well as keep versioning history.
FRQ015	M	The FCMS shall provide a functionality for management of the documents' templates.

Requirement's Identifier	Type	Explanation
FRQ016	M	The FCMS must generate and assign unique IDs to every file uploaded in the System as well as for the documents generated by FCMS.
FRQ017	HD	The System will provide a „Preview in PDF" functionality that must allow users to preview any document generated by the System before its saving or printing.
FRQ018	M	All the cases in the System, after being initiated, are distributed (allocated, assigned) to the relevant departments and experts, according to the workflows/procedures in force.
FRQ019	M	The distribution of any case shall involve the designation of at least the responsible Case Supervisor and responsible expert. A case may involve many experts in case of a complex judicial expertise.
FRQ020	M	The FCMS must keep registries of the accredited forensic experts and their association with certain forensic institution(s).
FRQ021	M	The System must keep in its DB the configuration of the experts and departments for each of the involved forensic institution. When the case distribution process will be launched for a certain case in a forensic institution, the System will consider automatically only those departments, laboratories and experts, as well as other users pertinent to the respective forensic institution. i.e. The System MUST NOT allow the assignation of an user as responsible expert if this expert is not employed in the forensic institution which received the original request/application and which is responsible for the said expertise case.
FRQ022	M	The System will provide two ways for receiving and attaching documents to a case: By receiving paper-based documents through the secretariat-related subdivision of the forensic institution; Scanning of the document; Uploading it into the System and filling all necessary metadata about the received document; and attaching the uploaded document to certain case; or By receiving electronically signed documents from other

Requirement's Identifier	Type	Explanation
		involved actors such as Prosecutors, Courts, etc. This approach may involve the receiving of documents from other ICT systems e.g. PIGD or e-File System of the General Prosecutor Office.
FRQ023	M	The FCMS must support the business-processes workflows configuration (BPM) tool. It should provide also a dedicated form designer which shall allow the System Administrators to (re-) configure the relevant electronic forms as per the business-processes. FCMS must allow (re-)configuring of the case management workflows for each forensic institution separately.
FRQ024	D	The FCMS software solution must provide features concerning the user interface customization. The functionality should allow the user to individually create own profile, to configure and preview the workspace's components order in such a way that makes the most sense for work.
FRQ025	M	The FCMS must provide an administration interface that allow users to access the System's settings as per their roles and rights.
FRQ026	M	The FCMS must provide archiving capabilities. Users from the forensic institutions must have the possibility to archive the entire case (which may include files, reports, data) according to the workflows and procedures in force.
FRQ027	M	All the modules of the System must reflect the method of organization of the judicial expertise process by involving the relevant actors/users.
FRQ028	M	The FCMS software solution must be fully integrated so that at the validation of a transaction, the data is updated and validated in all related modules.
FRQ029	M	The structure of the FCMS's components must be designed so that the legislative or organizational changes which may intervene afterwards can be operable with minimal efforts by the System Administrator.
FRQ030	M	The FCMS must contain a configuration feature, which allows the shared access of the users to the System resources, by definition of user roles at the level of module, function and operation.

Requirement's Identifier	Type	Explanation
FRQ031	M	The FCMS must allow the delimitation of responsibilities of each user role up to the level of function/operation (configuration of roles at level of menu, module, function, operation, action).
FRQ032	M	The FCMS must be able to provide simultaneous access of assigned users from different forensic institutions to a certain case.
FRQ033	M	The FCMS must be flexible, being able to use a range of parameters which are established depending on specific requirements of each forensic institution;
FRQ034	M	For the protection against deliberate or accidental attempts of unauthorized access to the data it stores, the FCMS must assure: • Security of data via System limitations of access based on rights and passwords, broken into several levels; • For a user or group of users, the configuration of rights of access must be possible only from the interface of the application; • The logging of daily operations individually for each user with right of access to the change of entries, with marking of the time when each operation was executed and the identity of the user who initiated it.
FRQ035	M	In order to assure the coherence of data, the FCMS shall use the principle of processing transactions so that in case of an accidental breakdown of the System all the completed transactions shall be permanent and those uncompleted shall be cancelled;
FRQ036	M	The FCMS must assure the integrity of data by checking the inconsistent data (checking and validation), missing data (validation) or deteriorated data (checking of inconsistency and validation of business-rules functionally implemented in the System).
FRQ037	M	The FCMS solution must allow the configuration of logging of transactions of users, at application level.

10.3. Functional Requirements to the "Management of Cases" component

Requirement's Identifier	Type	Explanation
FRQ038	M	The System will generate and assign a unique identification (ID) number to each case during the initiation process. This unique ID will be kept during the entire lifecycle of the case and even after the archiving. The System must ensure the traceability of the case's documents based on IDs.
FRQ039	M	The Registrar who is responsible for application's registration must have the possibility to add all necessary metadata related to the request/application and the Requester/Applicant. The FCMS will not allow initiation of the case until all mandatory metadata are provided.
FRQ040	M	The distribution of the cases to the responsible department and assignment of the case supervisor and responsible expert must be implemented according to the described business-processes (in this document) but also by taking into account the specifics and opinion of the involved forensic institutions. The process of cases' distribution must be configurable separately for each forensic institution.
FRQ041	M	The System must track the deadlines by taking into account each major stage of the case's lifestyle. Specifically, the System may alert the Manager or a Case Supervisor if their action is required prior the deadline expiration. The aforementioned deadlines must be configurable by the System Administrator, separately for each of the forensic institutions.
FRQ042	M	The System must be able to generate the list of pending tasks for each user depending on his role in the case and the given moment in the workflowjudicial expertise .
FRQ043	M	The distribution process shall take place for every case.
FRQ044	M	Before accepting a case for a properly expertise process the forensic institution must be able to check whether the relevant payment for the judicial expertise services has been received. This can be done through the following two options: • Integration with electronic payment gateway "MPay". This option involves the prior issuance of the invoice to the requestor by using "MPay"; • Granting access to the System to a user from the forensic institution who will have the right to indicate manually whether

Requirement's Identifier	Type	Explanation
		the payment for certain case has been received or not.
FRQ045	M	The following users: Registrar, Manager and Case Supervisor, are responsible for the case initiation in the System. Until the moment of selecting the responsible expert and other experts to be involved, if any, no other users can have access to the information, data or files from the respective case. The assignation of the responsible expert in the System can be done by the Manager or Case Supervisor. As the expert may be indicated directly in the request/application form and subsequently filled by the Registrar in the System, FCMS may suggest the respective expert as required by the Requester, but the decision and the operation in the System shall be made by the Manager or alternatively by the Case Supervisor.
FRQ046	M	The System Administrator must have the possibility to (re)configure the workflow for selecting and assigning of the involved expert(s).
FRQ047	M	The FCMS must be able to manage the complex and pannel judicial expertise cases. There may be cases, when a judicial expertise will involve several experts, even from different forensic institutions. In any case, one of the forensic institutions shall be the coordinator/responsible of the forensic case.
FRQ048	M	If several experts are involved in a forensic case, the System shall allow drafting of the forensic report's parts which are relevant to each expert.
FRQ049	M	The System shall allow an expert to request and initiate a laboratory investigation. In such a case, the System shall create a new folder attaching the request and other laboratory-related documents and data, including the laboratory's final investigation report. The laboratory investigation report shall be signed by the responsible expert from the laboratory and attached to the original case (the case which requested the laboratory investigations). In order to realize the aforementioned activities, the Contractor shall undertake all necessary business analysis activities to identify and analyze the relevant documents' forms, reports and data that are processed by the laboratories of the national

Requirement's Identifier	Type	Explanation
		forensic institutions. The relevant workflows, related documents, information, data, and reports circulated within forensic laboratories must be digitized into the new FCMS.
FRQ050	M	The System must take into account the availability and workload of each expert during the process of case distribution. There might be cases when the expert required by the Requester is not available due to i.e. regular or medical leave or high level of workload. In such cases the System shall exclude such experts from the distribution process and show the relevant explanation.
FRQ051	M	Once the distribution process is finalized and all experts of are selected, the System will send automatic alerts/notifications to all selected users and all of them will have access to the case's files.
FRQ052	M	The responsible experts may have full access to the information, data and documents of a case, while the Manager and Case Supervisor may have read-only access.
FRQ053	M	During the process of filling of the electronic form related to certain case – the System shall check the correctness of the provided data by the user through validation procedures. The validation may involve both: client-side and server-side validations.
FRQ054	M	Any case, after its finalization (which includes issuing of the forensic report and returning of the evidence to the requestor) must archived. The access to any information, data, document or report from an archived case MUST be restricted to all users, including the responsible expert who is the author of the judicial expertise report.
FRQ055	M	The access to the archived cases may be granted through a special procedure which includes the mandatory approval of the Manager of the forensic institution. This kind of operation shall be strictly documented and logged into the System. The exact data which shall be recorded and stored during such a procedure will defined during the Analysis and Design Phase of the project with the involvement of the relevant subject-matter expert from the national forensic institutions.

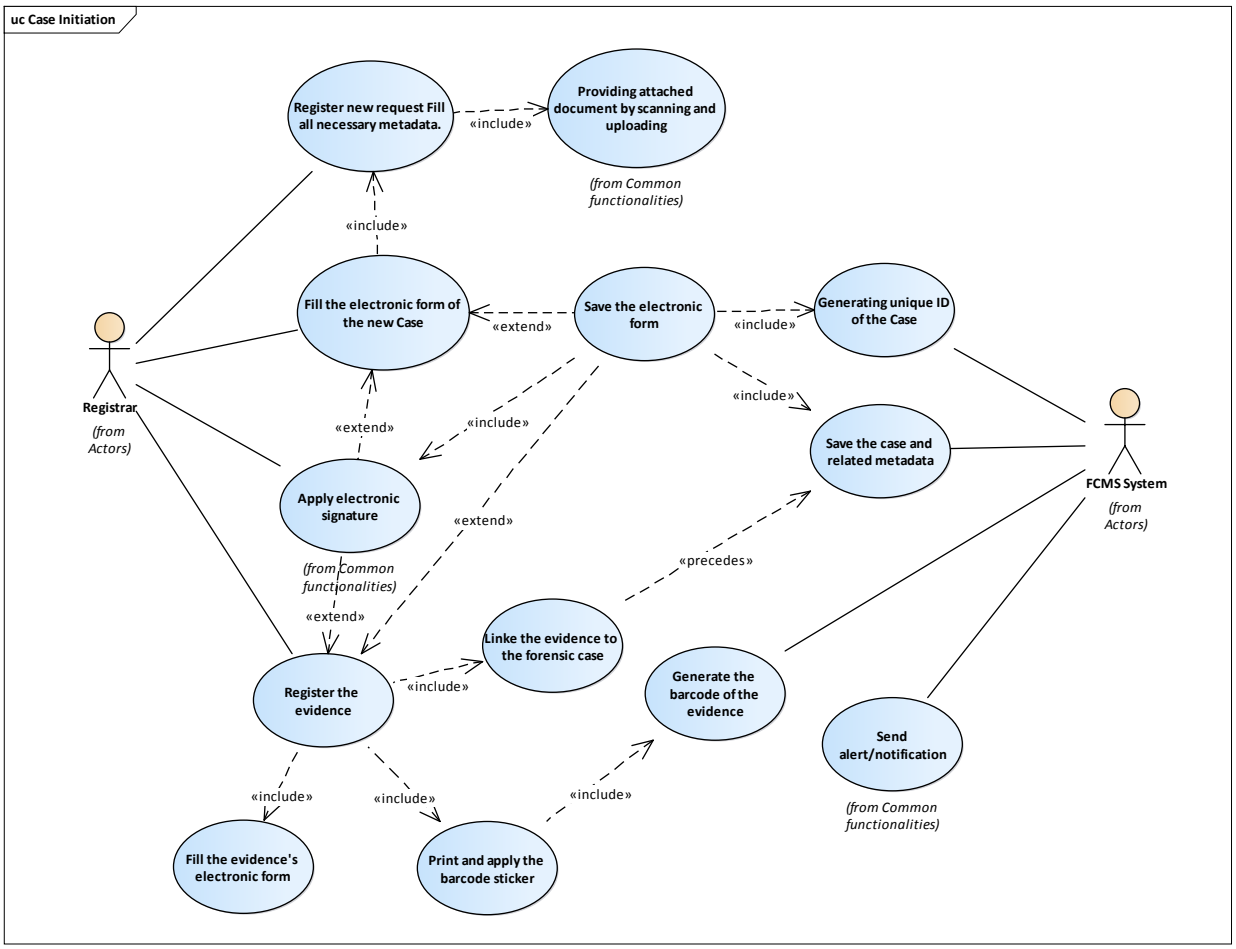


Figure 2. Use Case diagram related to the initiation of a forensic case

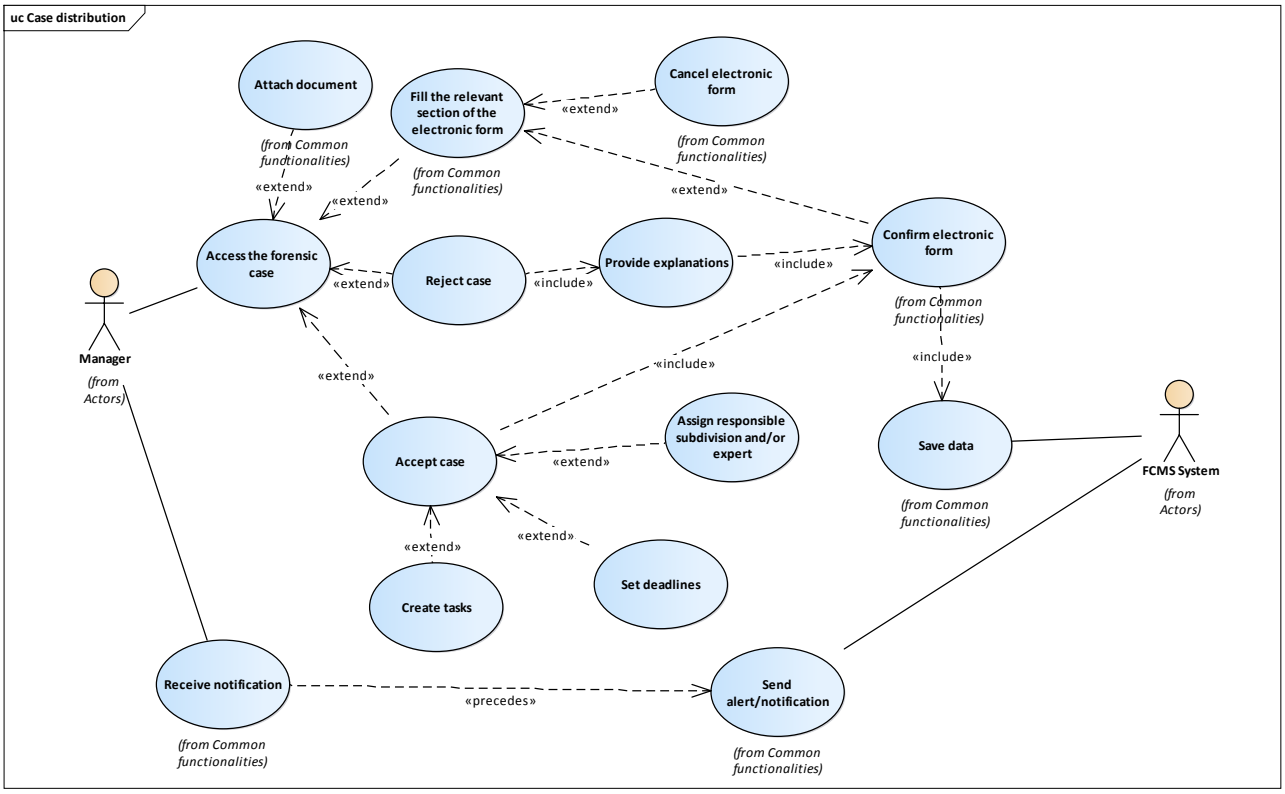


Figure 3. Distribution of cases by the Manager

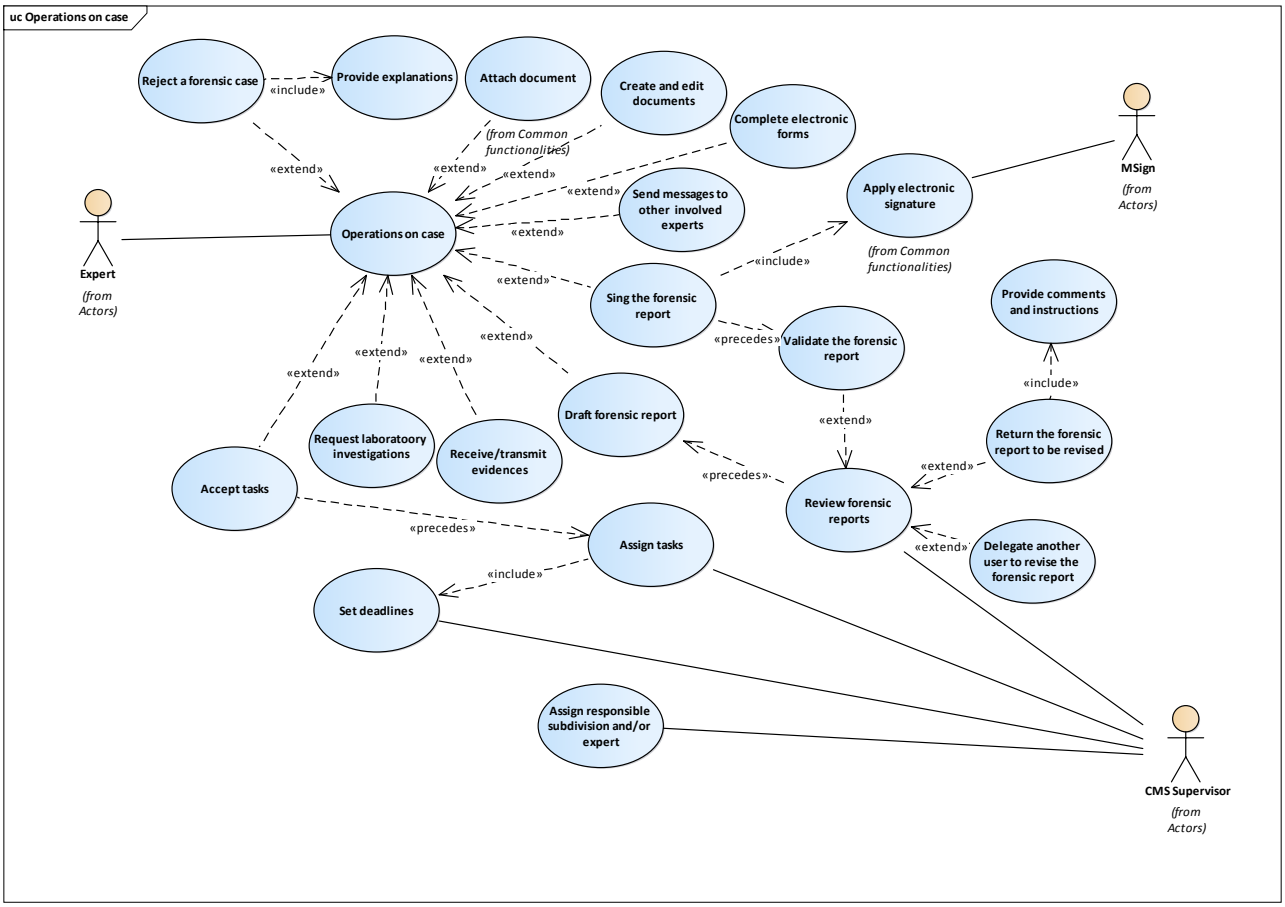


Figure 4. Possible use cases related to the judicial expertise processes

10.4. Functional Requirements to the "Evidence Management" component

Requirement	Type	Explanation
FRQ056	M	Evidence management component, packs a group of activities and processes related to handling objects to be investigated in the context of forensic and judicial expertise (evidences). Each forensic institution keeps and tracks evidences based on their internal operation procedure; however, the processes are more or less similar, the major difference being in forms of the documents and data fields used. The specific characteristics of each forensic institution shall be established during the Analysis and Design Phase. In this regard, the FCMS shall provide functionalities for managing evidences by providing a dedicated repository, which would foster at least the following possibilities: • Search and retrieval of evidences from the storage facilities; • Managing of the data describing the evidence; • Accessibility of evidence, whether it's in warehouse or in

Requirement	Type	Explanation
		work in certain department; • Reporting and auditing of evidence lifecycle; • Evidence tracking by using barcodes.
FRQ057	M	The FCMS must provide a barcode generator function to be used when registering new evidence. The exact method of barcode handling shall be designed during the Analysis and Design Phase of the project.
FRQ058	M	The functionalities related to the evidence management shall be derived from the described business-processes in this document. However, the following main stages can be mentioned that take place during the lifecycle of a judicial expertise case: • Evidence registration – usually take place at the moment of receiving of the request/application from the Requestor; • Evidence dispatch to internal department/laboratory of a forensic institution; • Returning of the evidence to requestor.
FRQ059	M	The System shall provide a specific electronic form for recording all the data about the evidence during its registration. Also, during the registration process, the System shall generate and assign a unique identification code by using barcodes. The respective barcode shall be printed by the user by using a barcode printer and the sticker with the code shall be applied on the object pack. The aforementioned identification code cannot be changed during the lifecycle of the forensic case. It must be mentioned that there may be cases when certain evidence (object) cannot be submitted physically to the forensic institution e.g. buildings, cars, etc. Even in such cases the information about the object shall be registered into the System, including the address where the object is located.
FRQ060	M	Any manipulation with the evidence (object) must be performed by users by using barcode scanners and completing the relevant electronic forms about the operation. The evidence can be dispatched to certain department of the forensic institution or laboratory or to a specialized warehouse. All kind of actions related to the evidence shall be recorded into the System in order to ensure the chain of traceability.
FRQ061	M	Every evidence registered into the System (FCMS) shall be linked to a case. There are no situations when an object (evidence) can be without a case.
FRQ062	M	The System must be able to identify the case and all other related information and data (e.g. requestor, responsible expert, deadlines, etc.), after scanning of the evidence's barcode.

Requirement	Type	Explanation
FRQ063	M	Under no circumstances a case can be closed (finalized) or archived if the evidence was not returned to the requestor.
FRQ064	M	During the process of filling of the electronic form related to operations with evidences – the System shall check the correctness of the provided data by the user through validation procedures. The validation may involve both: client-side and server-side validations.
FRQ065	M	The users must have access to the information related to certain evidence only according to their rights and role in the case.

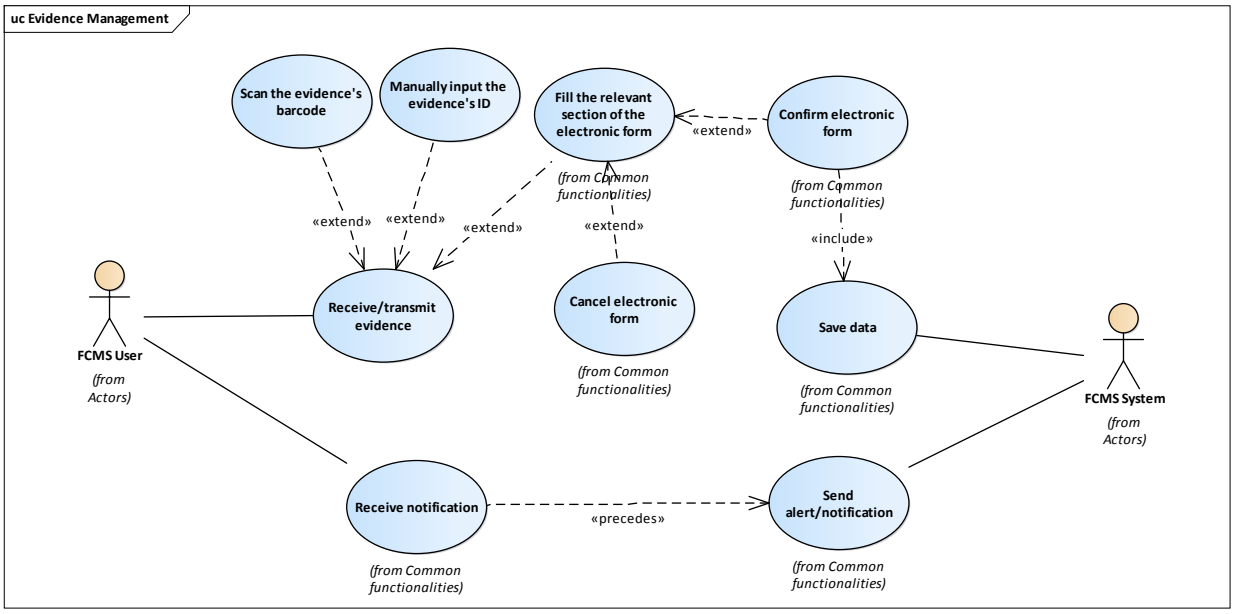


Figure 5. Use Cases related to the evidence management

10.5. Functional Requirements to the Document Management component

Requirement's Identifier	Type	Explanation
FRQ066	M	The FCMS must allow uploading of files and assigning them to forensic cases. Also, the System shall be able to manage incoming and outgoing documents that are not part of certain forensic cases.
FRQ067	M	The System must able to generate documents (in .PDF format) based on predefined document templates and data from database.

Requirement's Identifier	Type	Explanation
FRQ068	M	The FCMS must provide the possibility of creating dynamically folder structures in a case.
FRQ069	M	The FCMS must provide the functionality of creating documents from MS Word template.
FRQ070	M	The FCMS must provide document collaboration capabilities, so the user be able to provide comments during sending/receiving a document.
FRQ071	M	The FCMS MUST NOT allow a document to be deleted from the forensic case. The user may mark a document as canceled or deleted and the System can make it inactive, but the document shall never be deleted. The editing of the documents is allowed until the case is finalized and closed.
FRQ072	M	The System must provide Draft or Final document statuses.
FRQ073	M	The FCMS must enable automatic saving of the information related to actions carried out by users while working with the document from a case.
FRQ074	M	The FCMS must allow the approval of documents by using electronic signature, through the integration with MSign e-service.
FRQ075	M	The FCMS must provide the functionality to initiate workflows automatically and add the respective documents, according to the configured business-process.
FRQ076	M	The System must be able to provide the entire traceability of actions related to a document.
FRQ077	M	The FCMS solution should support an optional folder structured naming mechanism which includes names (e.g. personal or corporate names).
FRQ078	M	When creating a new electronic folder in a classification scheme which uses a structured numerical or alphanumerical reference, the System shall automatically generate the next sequential number available at that position within the scheme.

Requirement's Identifier	Type	Explanation
FRQ079	M	The FCMS solution must not, by its own architecture or design, impose any practical limit on the number of folders that can be created under any forensic case, or within the entire System.
FRQ080	M	The FCMS must support the use of metadata for folders and must be capable to restrict the addition or amendment of metadata elements to authorized users.
FRQ081	M	The FCMS must support inheritance of metadata by folders allocated to a case so that, by default, addition of a new folder results in automatic inclusion of those attributes which derive from the case to which it is allocated.
FRQ082	M	The FCMS solution must be capable to provide configuration features so that the ability to create new folders can be controlled according to the user's role.
FRQ083	M	The FCMS must prevent the destruction or deletion of an electronic folder or entire case and any of its records or metadata at all times.
FRQ084	M	The FCMS must allow a case's folder or group of folders, and all parts and records that fall under that folder(s), to be re-classified, by an authorized user, to a different point in the classification scheme, and should retain a history of their location prior to re-classification.
FRQ085	M	The FCMS must ensure that all electronic records and part(s) remain correctly allocated following the relocation of a folder or group of folders, so that all previous structural links between records, parts, and folders are retained.
FRQ086	M	The FCMS should allow all relevant folder and record metadata attributes which are determined by the point in the classification scheme (including those determined by inheritance) to be, optionally, automatically updated following the re-location of a folder.
FRQ087	M	The FCMS must offer functionalities for automated archiving of documents that are printed or created as a PDF. The relevant rules must be possible to be configured by the user (e.g. System Administrator) in order to assure the processes to run automatically.
FRQ088	M	The FCMS must provide automatic versioning capabilities to track changes of the documents, including information about users performing certain actions using major and minor versions of

Requirement's Identifier	Type	Explanation
		documents.
FRQ089	M	The FCMS must provide the functionality for co-authoring of documents, meaning multiple users can work on a single document at the same time. This can be also the case of drafting of the judicial expertise report.
FRQ090	M	The FCMS will provide functionality for making comments on the documents' flows. Also, it must be possible to add comments to each version of the document.
FRQ091	M	The FCMS must be able to manage and allocate resources for each activity in the workflow for processing a case. Specifically, the System will automatically generate users' tasks that represent a workflow element. FCMS users must be able to create tasks, assign tasks to other users or a group of subordinates, and delegate tasks to other users/user groups.
FRQ092	M	The FCMS must enable the creation of subordinated tasks (creating new tasks on the basis of an already existing tasks) and to manage the relationships between them.
FRQ093	M	The task management capabilities of the FCMS must provide a notification (through e-mails and reminders) to alert users about the deadline of a task that needs to be accomplished. Also, the System shall inform users, via the Dashboard about the critical tasks.
FRQ094	M	The System must allow the user to define the link between the incoming and outgoing documents. e.g. This is necessary in order to ensure the communication between the requestor and the forensic institution, when the questions/answers are issued/received in the forms of letters.

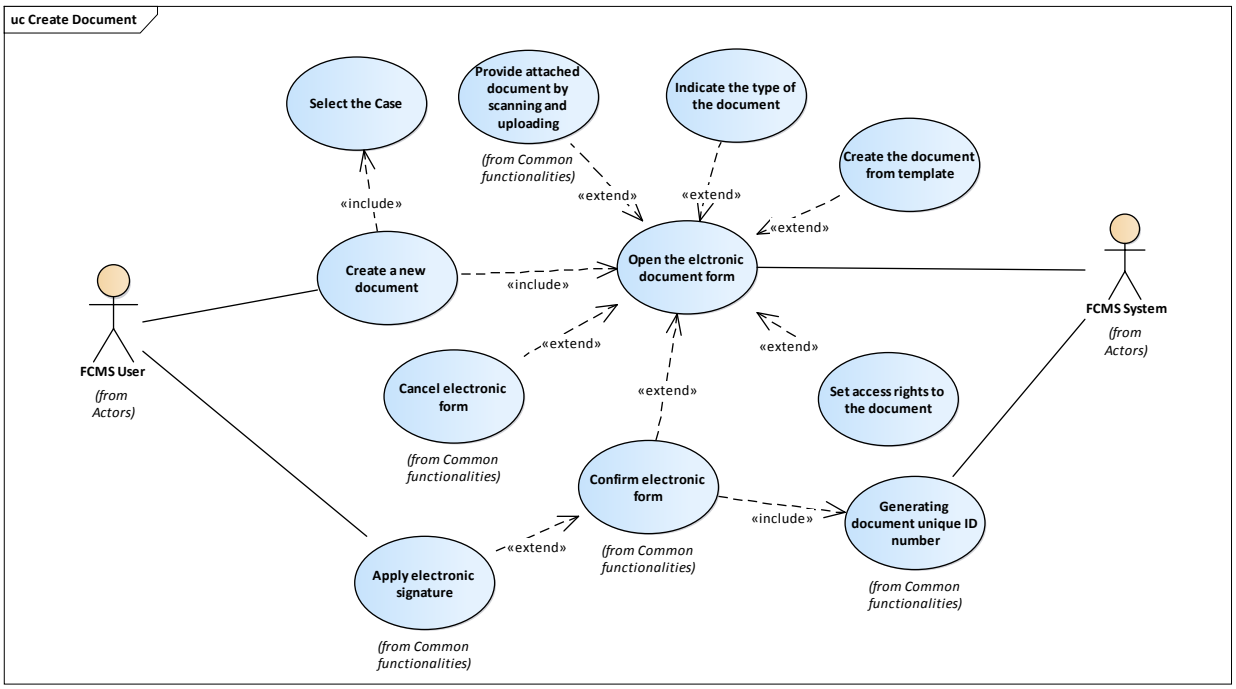


Figure 6. Possibilities regarding the creation of a document into the System

10.6. Functional Requirements to the Notifications and Alerts capabilities

Requirement's Identifier	Type	Explanation
FRQ095	M	This component of the System shall realize the appropriate notification of the actors depending on their role and event.
FRQ096	M	Any user in the FCMS could be alerted if a certain deadline set for one of his tasks is about to expire.
FRQ097	M	The means and mechanisms for notification / alerting can be, for example: e-mail messages, notifications via the user's workspace dashboard or by using MNotify governmental service. The details shall be decided during the Analysis and Design Phase together with the forensic institutions.
FRQ098	M	This component shall be used also for notifying requestors about the status of their submitted applications (requests for judicial expertise).
FRQ099	M	The notification and alerting mechanism must be configurable. The System Administrator will have the right to configure it.

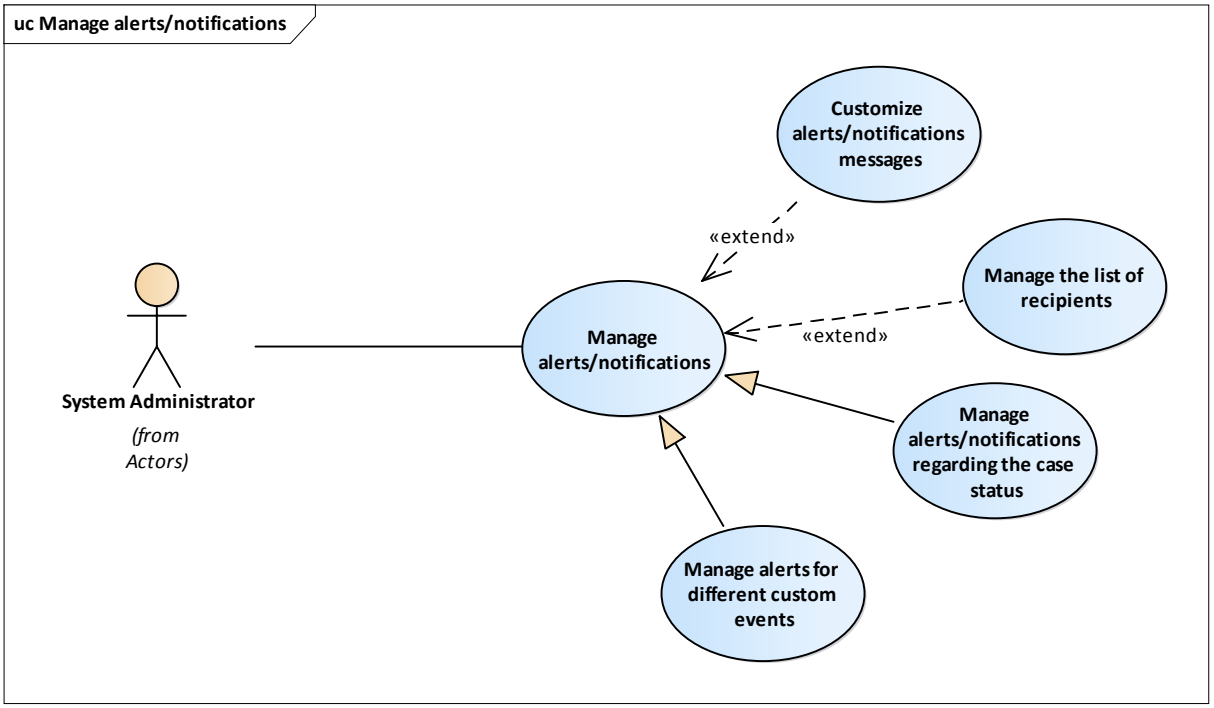


Figure 7. Management of Notifications and alerts

10.7. Functional Requirements to the Reporting component

Requirement's Identifier	Type	Explanation
FRQ100	M	The FCMS solution must provide a reporting tool in order to support the analytical and decision-making progress. Therefore, the System shall be able to generate reports based on any data stored in its database that are related to the judicial expertise cases regardless of their status. FCMS shall provide various reporting formats, such as tabular format or graphical representation and the users must be able to select the type/format of each report to be generated. A list of reports that shall be implemented in the System will be defined during the Analysis and Design Phase together with the beneficiary institutions.
FRQ101	M	The FCMS must be able to generate reports based on available data by different topic (e.g. expertise type) with the possibility of customization of views of analysis (table or graphic).
FRQ102	M	The proposed solution must allow users to establish filtering and sorting criteria at the moment of running reports. Also, the FCMS reporting tool shall allow users do design customized reports and save their templates. In addition, there must be possible

Requirement's Identifier	Type	Explanation
		to generate ad-hoc reports.
FRQ103	M	The FCMS solution must allow the generation of synthetic reports with aggregated data.
FRQ104	M	The FCMS must allow the use of schemes of fast definition of requirements of each specific data field (field covered by the System).
FRQ105	M	The FCMS must allow the generation of reports in real time per each involved forensic institution. Each forensic institution may have access only to those reports that contain data on cases in which the institution was or is involved. In other words, a forensic institution cannot have access to the reports that contain data about the cases processed by another forensic institution.
FRQ106	M	The FCMS must assure the possibility of adding new types of reports in a simple and intuitive manner.
FRQ107	M	The FCMS must allow the generation of any types of reports (e.g. analytical, statistical) depending on requirements.
FRQ108	M	The reports must be exportable in PDF, MS Excel formats. Also, the System shall provide an automated delivery mechanism of reports (e.g. through e-mail). In this sense, the FCMS will provide support for subscribing to reports for the forensic institutions' users, by receiving generated reports by e-mail at certain time, configured based on the criteria defined by the subscribed user.
FRQ109	M	The FCMS shall allow definition of templates containing, at least, a header and footer of the forensic institution and other general information.
FRQ110	M	The FCMS shall allow creation, change or deleting of generated reports, also allowing: saving settings for further use.
FRQ111	M	The FCMS reporting tool must support the design/development of an unlimited number of reports.
FRQ112	M	The reports shall be provided with filter by fields function (e.g. Period, forensic institution, type of expertise, etc).
FRQ113	M	The reports' columns / information will be displayed based on list of fields from the System's database (relational or multidimensional),

Requirement's Identifier	Type	Explanation
		with the possibility to specify their type and size. It shall be also possible to apply the list of possible operators: • Totals / subtotals - based on a list of fields from the database and a list of possible functions or operators; • Possible filters - based on a list of fields from the database; • Default filters/conditions - the field and the value to be specialized; • Ordering - based on a list of fields from the System's database (relational or multidimensional).
FRQ114	M	The report shall contain a pre-defined name for export in another format.
FRQ115	M	The reporting shall be visualized through a web-browser without the need to install other additional software.

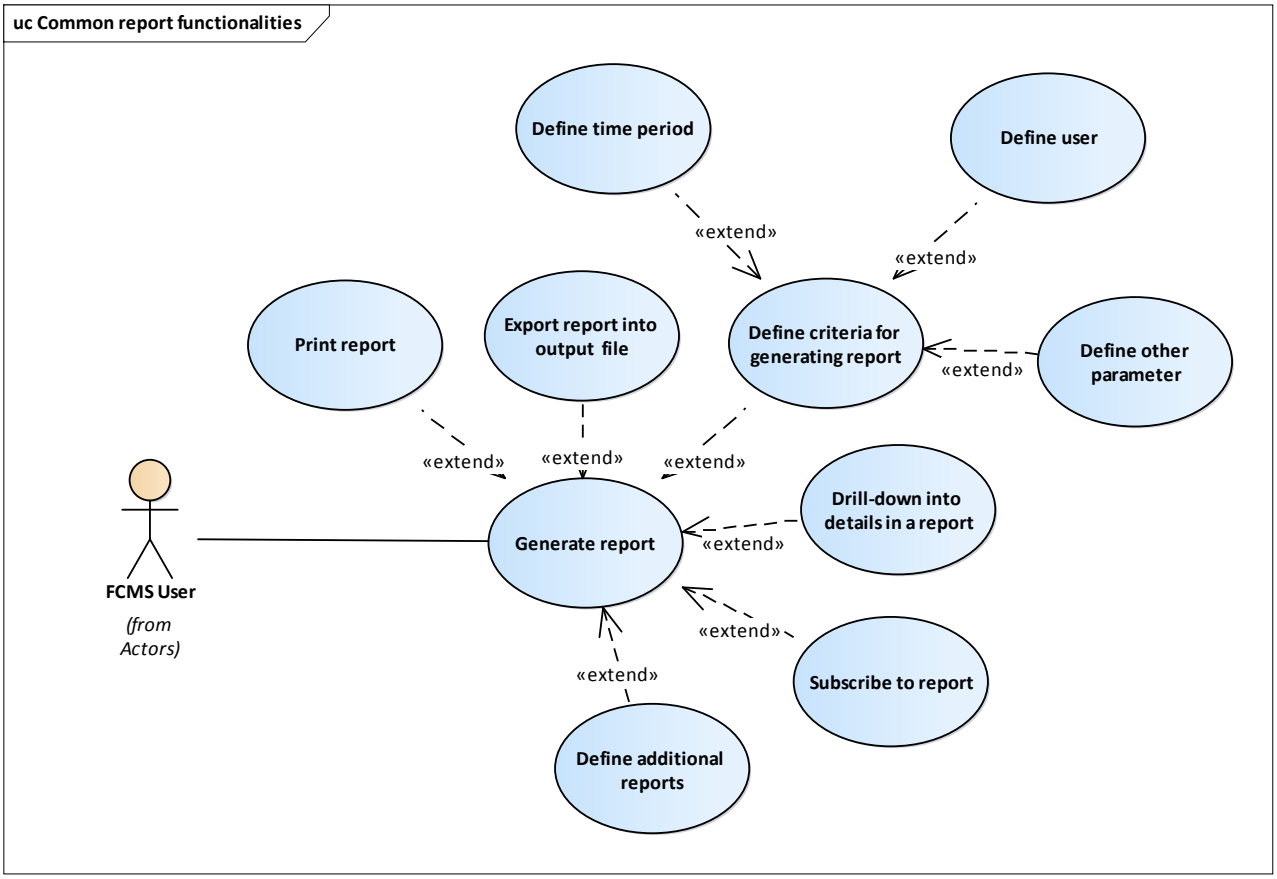


Figure 8. General Reporting Functionalities

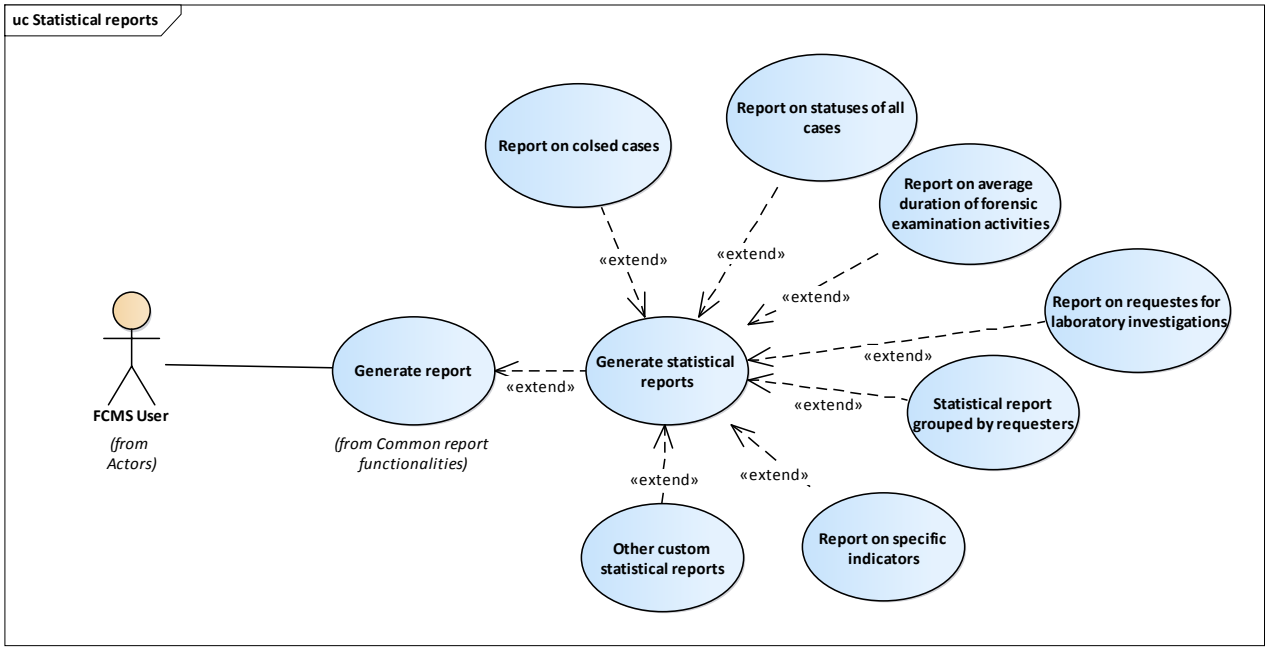


Figure 9. Examples of statistical reports

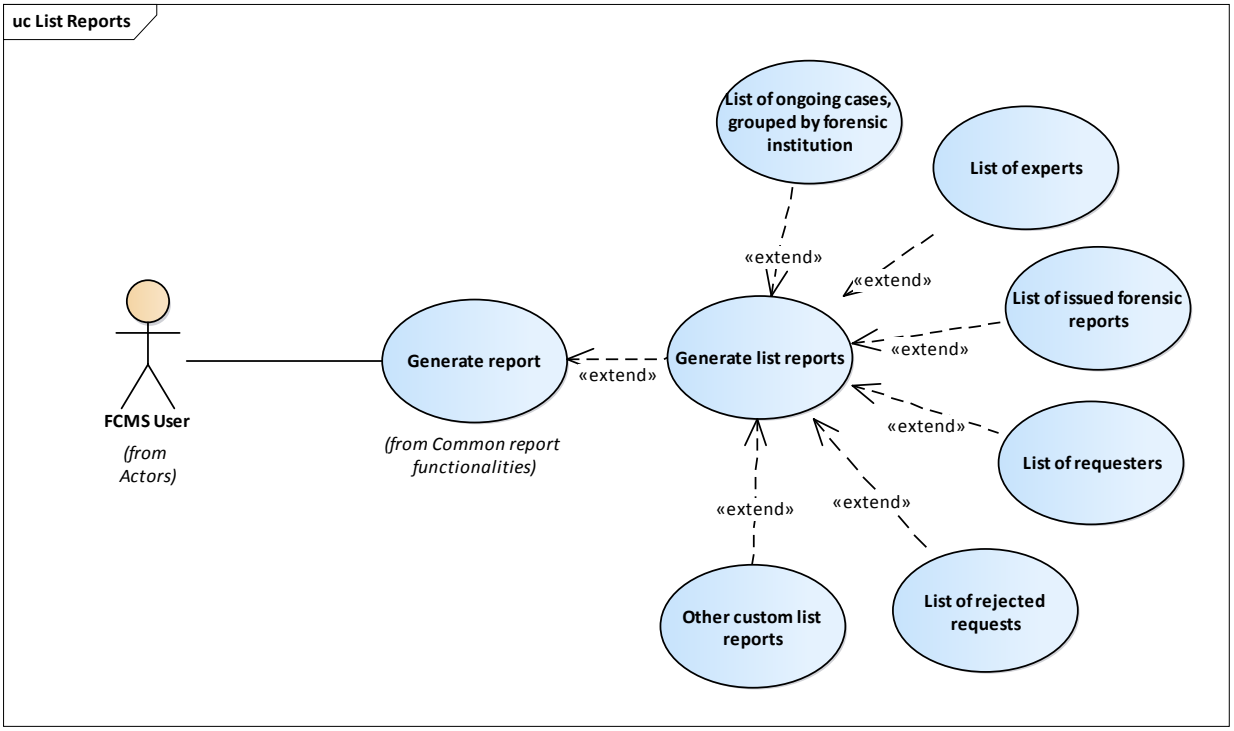


Figure 10. Example of List reports

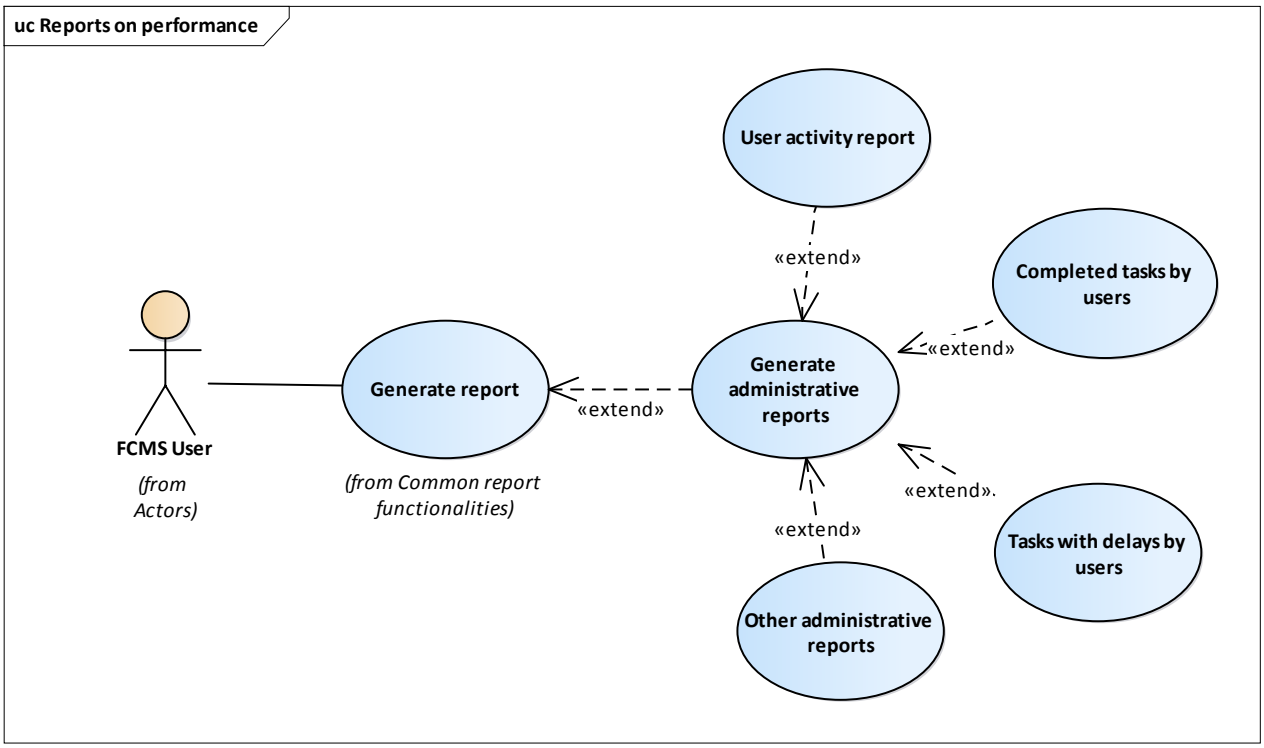


Figure 11. Reporting on performance

10.8. Functional Requirements to the Searching and Filtering capabilities

Requirement's Identifier	Type	Explanation
FRQ116	M	These functionalities must provide to the users a powerful tool for searching and retrieving information related to the judicial expertise cases registered in the System.
FRQ117	M	The FCMS must allow the retrieval of information by indicating the specific criteria of the searched subject, such as: "type of judicial expertise ", "requestor", "year/month/date", "forensic institution", etc. The user shall be able to indicate one criterion or a combination of criteria according to which the System shall perform the search and must display on the screen the list of results found.
FRQ118	M	Any information found and displayed on the screen regarding forensic cases must be possible to be filtered by the user based on the filtering criteria. In this sense, the FCMS shall support filtering of cases according to the period of time, expertise type, department/laboratory, etc. Also, the System should support defining multiple filters (e.g. forensic institution, etc).
FRQ119	M	The FCMS shall allow searching and filtering the documents according to diverse criteria, such as registration date, period of time, type of document, sender, etc.
FRQ120	M	The FCMS shall allow searching and filtering of involved forensic experts. e.g. the System will enable listing of all experts depending on their specialization and filtering them by the forensic institution.
FRQ121	M	The FCMS must also provide possibilities to sort the information found and displayed in tabular form. Thus, the information could be sorted ascending from A to Z (for columns containing textual values) and from 0 to 9 (for columns containing numerical values, e.g. amounts); or descending - from Z to A and from 9 to 0, as the case may be.
FRQ122	M	The system will provide the user with drill-down functionalities, so that selecting a record from the list of found projects will be able to delve into details to the most detailed level.

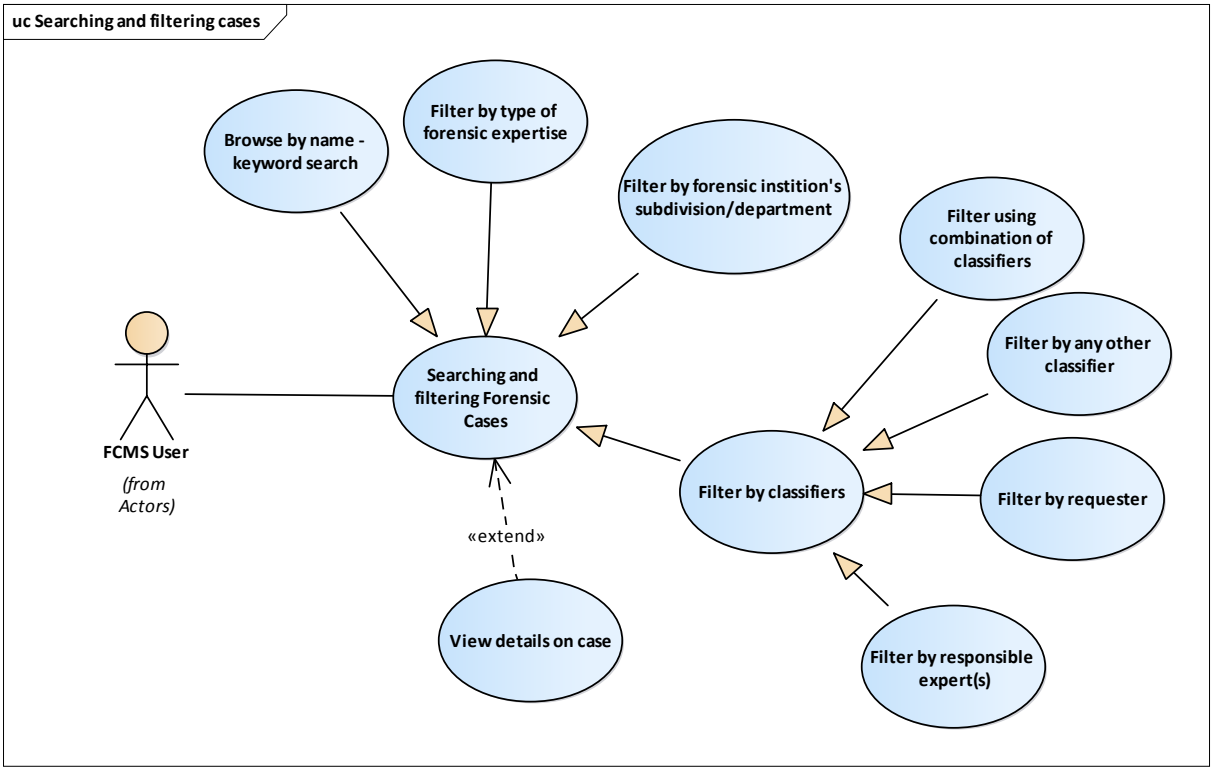


Figure 12. Searching and filtering of forensic cases

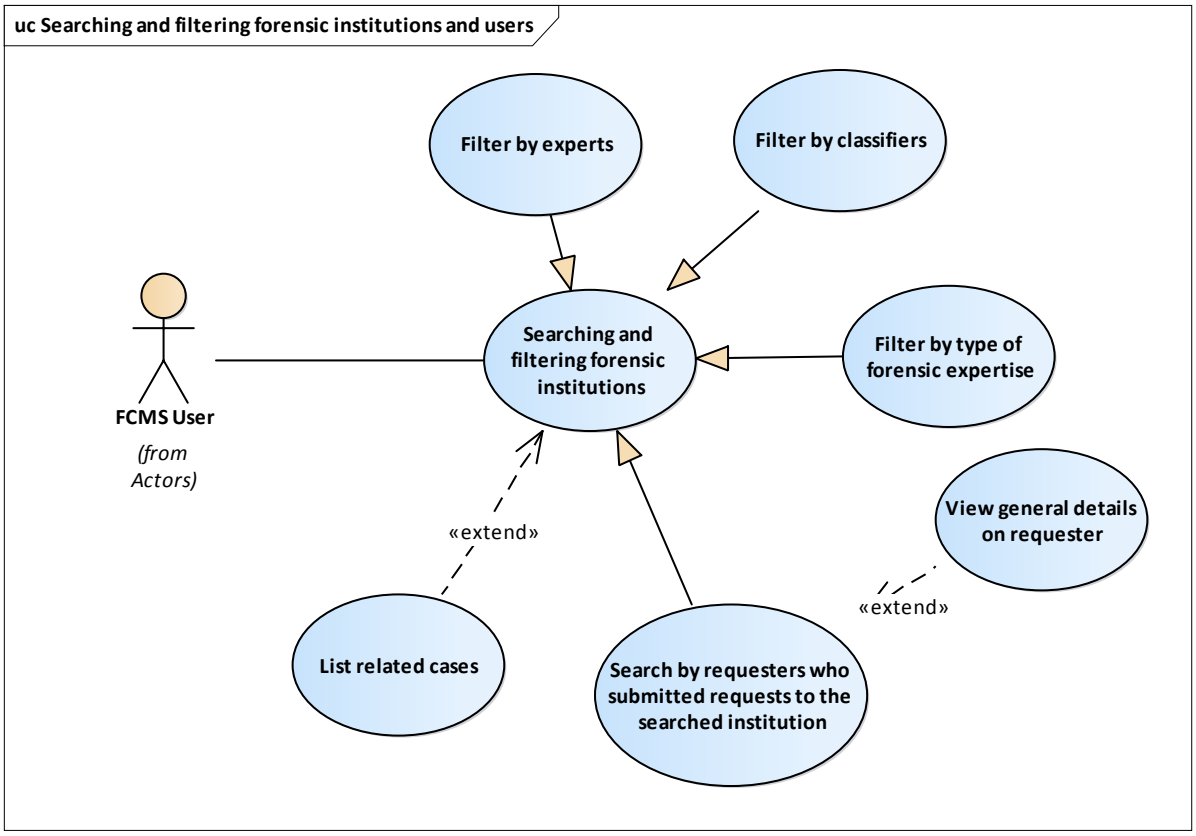


Figure 13. Searching and filtering forensic institutions

10.9. Functional Requirements to the System Administration

Requirement's Identifier	Type	Explanation
FRQ123	M	The System shall provide functionalities for managing the organizational structures of the involved forensic institutions. Thus, the System Administrator shall have the possibility to add, modify or deactivate any subdivision relevant to the management and record-keeping activities of the judicial expertise . The System shall not allow the elimination of the subdivision, if it is an active one, i.e. it is involved in certain processes or there are any documents, activities linked to this subdivision.
FRQ124	M	The System shall provide functionalities to the System Administrator for users' management. He must be able to attach roles to each user and necessarily indicate the subdivision where the user works.
FRQ125	M	FCMS shall provide the System Administrator with functionalities for managing users' roles and permissions. In this context, the Administrator will be able to set the necessary permissions: the level of access to data and the level of access to functionalities.
FRQ126	M	FCMS shall provide to the System Administrator functionalities regarding the management of classifiers. It must provide features such as "Add, Edit, Deactivate". Any classifier managed in the System will be unique for all project records.
FRQ127	M	FCMS shall provide to the System Administrator functionalities for configuring of the notification / alert mechanism. During the configuration of a notification / alert, the System shall offer the possibility to the System Administrator to indicate: • What is the event of the notification; • Who is the user to receive the notification; • Content (text) of the notification; • What is the time of notification; • Periodicity of the notification; • Other parameters

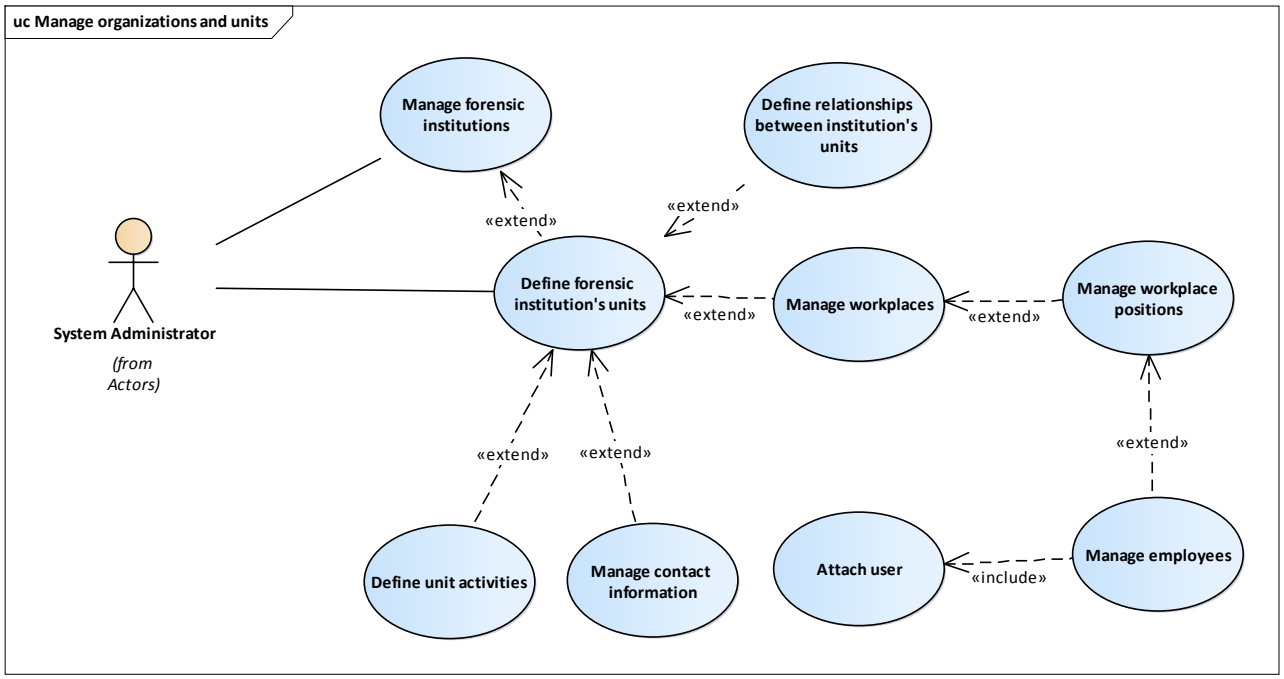


Figure 14. Management of the forensic institutions

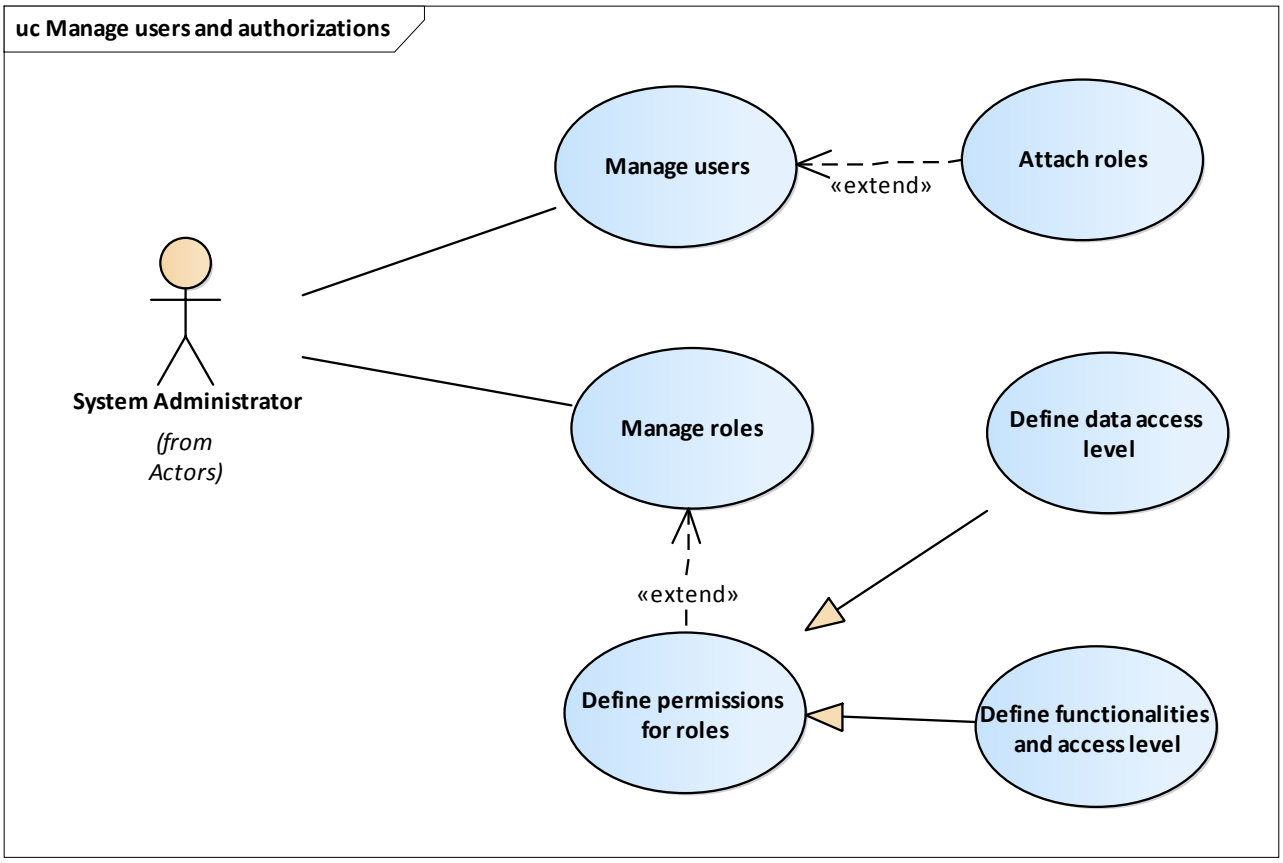


Figure 15. Users Management

11. Relevant Business-Processes

Following the analysis of workflows within the national forensic institutions, a business-process model has been developed which takes into account the use of an ICT tool (FCMS) in the daily activities of employees.

The proposed model involves a way of working aimed at using electronic documents and records, applying electronic signatures, using barcode printers and scanners to ensure strict keeping of records and custody of the evidences – objects subject to forensic examination, excluding manual filling of registries and forms on paper and by using special means of security, data protection and users' authorization.

The business-processes presented below were consulted with the beneficiary forensic institutions and subsequently agreed as a high-level business-processes model to be implemented within the FCMS.

11.1. Case Initiation

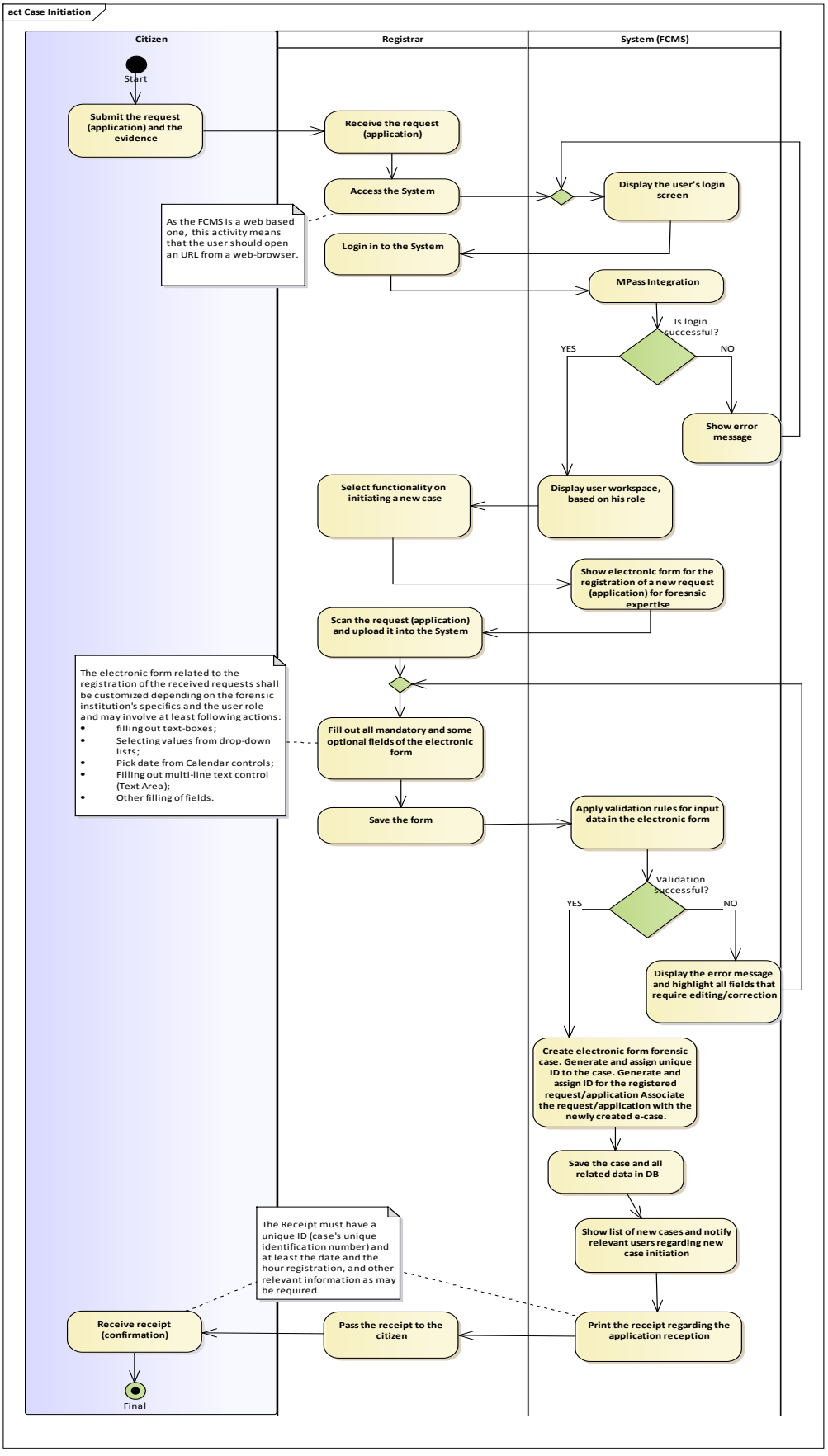


Figure 16. Case Initiation

The workflow for the initiation of the forensic case begins with the receipt of the request (application) from the Registrar. The request can be received on paper, in electronic format through e-mail or from another information system (e.g. ICMP (Courts), e-File system of the Prosecutor Office). Receipt of the request in electronic format requires it to be signed electronically.

The Registrar will access the FCMS through a web browser and will authenticate using the MPass service. If the authentication is successful, the System will redirect the user to the main page, which represents the user's workspace. It will contain at least a dashboard, which will present a quick summary of the current status of user tasks and the main menu.

Further, the Registrar will choose from the main menu the functionality of adding a new request in the System. In response, the System will display the electronic form that will enable the user to enter any information regarding the received request (application). It should be noted that that electronic form will transpose as much as possible the data fields of the paper sheets currently used by the forensic institutions, except some fields that could be pre-filled in by the System. They are to be defined at the stage of Detailed Analysis and Design of the System.

The Registrar shall scan all the pages of the received request and shall upload them into the System, while filling all the required data of the electronic form. The electronic forms to the forensic case shall be customized according to the specifics of the forensic institution and the user's role, and can involve at least the following actions:

- filling in TextBox elements;
- selection of values of the DropDown List elements;
- selection of values of Calendar controls;
- filling in the Text Area fields with text;
- uploading of files (e.g. PDF, JPG, etc.);
- other completions of fields, as appropriate.

Once the electronic form is filled, the Registrar will activate the 'Save' button and the System will trigger the validation process of the entered data. This can involve both Client-Side and Server-Side validation roles and processes. If incorrectly entered data are detected, the System shall display the relevant error message and will highlight the fields that are required to be edited/corrected. Once all the data have been entered correctly and all the validation rules have been successfully applied, the System will save the data and the request/application in the DB and will create the so-called 'electronic case', while generating and assigning unique identification codes (hereinafter: 'unique ID') for both the electronic case and the received request (application). The newly created case will be assigned the conventional status as 'New'.

Once the new e-case has been created, the System shall notify all relevant users about the initiation of a new forensic case by its available means (e.g. e-mail, SMS, user dashboard).

The System will propose to the Registrar to print, the receipt as confirmation of the request registration, which will be handed-over to the requester. It must contain at least the following data:

- surname, name of the requester or the requester's official representative;
- other data about the requester;
- date and time of registration in the System;
- unique ID of the e-case and request;
- surname, name of the Registrar;
- etc.

11.2. Primary registration of evidence – object of the judicial expertise

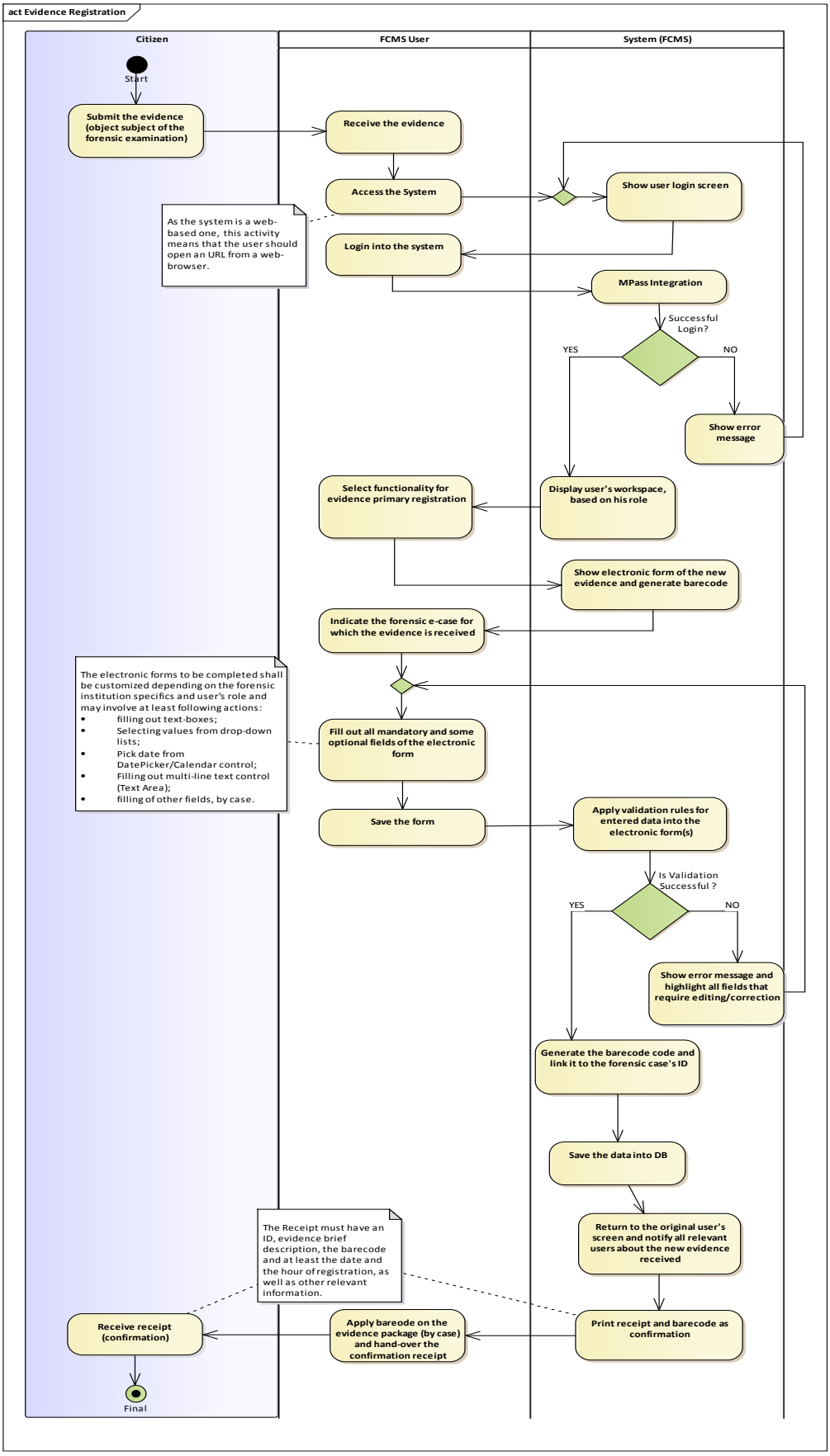


Figure 17. Receiving and registration of evidence

The flow of primary registration of the evidence – objects of the forensic examination will be implemented in the System through a set of features that may be assigned to different users, depending of the procedures of each forensic institution. This is necessary as in different forensic institutions, these activities can be carried out by different employees.

The role responsible for the registration, reception and release of objects may be combined with other user roles.

Thus, in the case of NCJE, this role can be assigned to an employee of the subdivision responsible for secretary activities, similar to POLICE FORENSIC CENTRE where it can be combined with the Registrar user role. This must not be a critical aspect for the FCMS ICT solution, as the System Administrator must be able to indicate which user may have access to such functionalities.

It should be noted that during the handling of the evidences, the proposed approach involves using of barcode scanners and printers.

Thus, the flow of evidence's primary registration in the System assumes that the user is successfully authenticated and authorized. He/she will access from the main menu the functionality of registration of a new evidence, and in response the System will display the evidence's electronic form, which can be pre-filled with certain data, i.e.: user's subdivision, date, time, etc.

Further, the user shall indicate the unique ID of the forensic case (or alternatively the ID of the received request/application), to which the received object refers, and shall fill in all other data fields of the electronic form. The electronic form may easily vary depending on the specifics of the forensic institution. Given that some fields that are relevant to certain forensic institution, at the same time may be irrelevant to another one. Completion of the electronic sheet of the received object may involve at least the following actions:

- filling in TextBox elements;
- selection of values of the DropDown List elements;
- selection of values of a Calendar control;
- filling in the Text Area fields with text;
- uploading of files (e.g. PDF, JPG, etc.);
- other completions of fields, as appropriate.
- indication of the appointed expert(s) in the request.

Once the data of the electronic form have been entered, the user will activate the 'Save' button and the System will trigger the validation process for the entered data. This can involve both Client-Side and Server-Side validation rules and processes. If incorrect entered data are detected, the System will display the relevant error message and will highlight the data fields to be edited/corrected.

After the correct entry of all data and after all validation rules have been successfully applied, the System will save the data into the database and will generate the barcode. The barcode shall be printed by the user using a special printer and subsequently the sticker with the barcode shall be applied on the package of the received object (evidence), depending on each case.

Once saved, all data about the evidence (object) will be linked with the respective ID (barcode), which must be unique and the System will be able to identify the object in the database at anytime. Any other operations related transmitting or receiving of the evidence from one subdivision to another, or from one user to another, will be performed strictly by using of barcode scanner, so that the System will automatically identify the evidence (object) and will record the operation in order to ensure the chain of custody of the object subject to forensic examination (expertise).

The System will propose the user to print the confirmation receipt of the evidence, which will be handed-over to the requester.

11.3. Acceptance and distribution of the forensic case

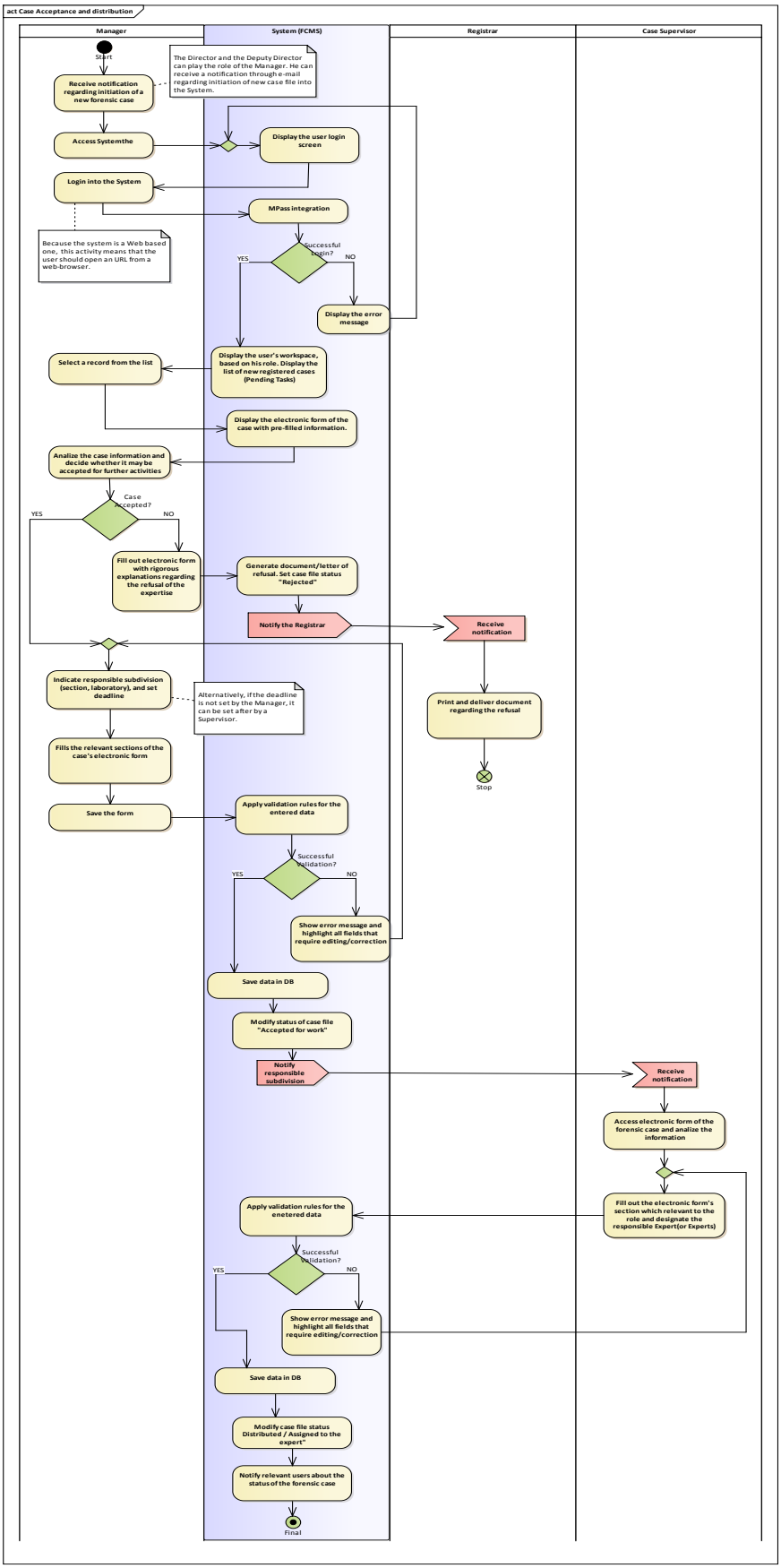


Figure 18. Acceptance and distribution of the forensic case

Once a new case is registered in the System, all relevant users will receive the corresponding notifications.

Thus, the user with the role of Manager will receive dashboard alerts (in the compartment of the pending tasks) and notifications in the form of e-mails.

The Manager will be able to access the list of pending tasks, either from the dashboard or from the main menu, and in response the System shall display on the screen the list of new tasks/cases that require the user's attention. Then, the manager will select the case from the list, and the System shall display the pre-filled electronic form of the case, which contains all the data about the case and related attached documents such as the received request (application).

After a careful review, the Manager will fill, if necessary, the section of the form which is relevant to his/her role and will indicate the subdivision responsible for carrying out of the forensic examination activities, as well as the deadline. Alternatively, if the deadline is not set by the Manager at this stage, it can be set later by the Case Supervisor. If an expert, other than that one indicated in the request, is appointed (if so needed), the manager is obliged to provide the appropriate explanations in the System, as well as to refer to the communication correspondence in terms of coordination with the requester about the replacement of the forensic expert.

This flow can also contain a decision-making activity, which can be active or inactive depending on the specifics of the forensic institution. Namely, the manager may have the possibility (after reviewing of the requirements to the forensic examination, the capabilities and resources needed to be involved) to refuse the forensic examination/case. In such a case, the System shall generate the rejection document (letter), in which the user must provide all relevant explanations. The document must be signed electronically and, if necessary, handwritten on paper, and subsequently sent to the requester through the role of Registrar.

The System will assign a unique ID to the rejection document and will attach it to the electronic case. Also, the System will automatically set the status ‘rejected’ to the respective case.

Otherwise, if the Manager has filled the relevant section of the case’s electronic form and indicated the subdivision and/or the responsible expert, the System will save the data into the DB and the status of the case shall be changed to ‘accepted/distributed to the expert’. The System shall notify the relevant users about this fact.

It should be noted that in some cases the manager could directly appoint the expert who will be responsible for the forensic examination. In such a case, the expert concerned will be notified that a new task is assigned to him/her.

The classic scenario assumes that the Supervisor, being notified by the System, will access the list of pending tasks from the dashboard of his/her workspace or from the main menu and will select the task. The System will display the electronic form of the case ensuring the access to the attached documents (request and any other document in the electronic case). The user shall review the information made available and will fill the section of the form that is relevant to his/her role, with the mandatory indication of the expert or experts to be involved. If the deadline for execution has not been set by the Manager, it can be set by the Case Supervisor at this stage.

If an expert other than that one indicated in the request is appointed, the user will have to provide explanations and the reason on the substitution of the forensic expert, as well as to refer to the correspondence with the requester. Completion of the electronic form may involve at least the following actions:

- filling in TextBox elements;
- selection of values of the DropDown List elements;
- selection of values of Calendar controls;
- filling in the Text Area fields with text;
- uploading of files (e.g. PDF, JPG, etc.);
- other completions of fields, as appropriate.

The System can also offer the so-called task management features, so that for all tasks assigned to experts, deadlines can be set for automatic tracking and sending alerts before their expiration.

The workflow management capabilities of the System must be able also to generate performance reports, presenting the number of assigned cases per each user, how many of them are delayed, how many of them are to expire soon, how many have already been completed, etc. This mechanism can provide the Manager and the Case Supervisor with relevant information and contribute to more effective decisions regarding the distribution of the effort within the

forensic institution. Of course, the setting of deadlines, as well as other task management parameters shall take into account several aspects such as: the type of forensic examination, available resources, etc. The System should also take into account the availability of forensic experts. For example, the System shall prevent the distribution of cases to those experts who are on leave (regular or medical). These details shall be identified later at the stage of detailed analysis and design.

Once the Case Supervisor has distributed the case to the expert(s), the System will change the status of the case and will notify the relevant forensic expert(s). At the same time, the requester can be notified about the change of the status of the case, through his/her Virtual Cabinet in the system or by e-mail.

11.4. Forensic examination and finalization of the case

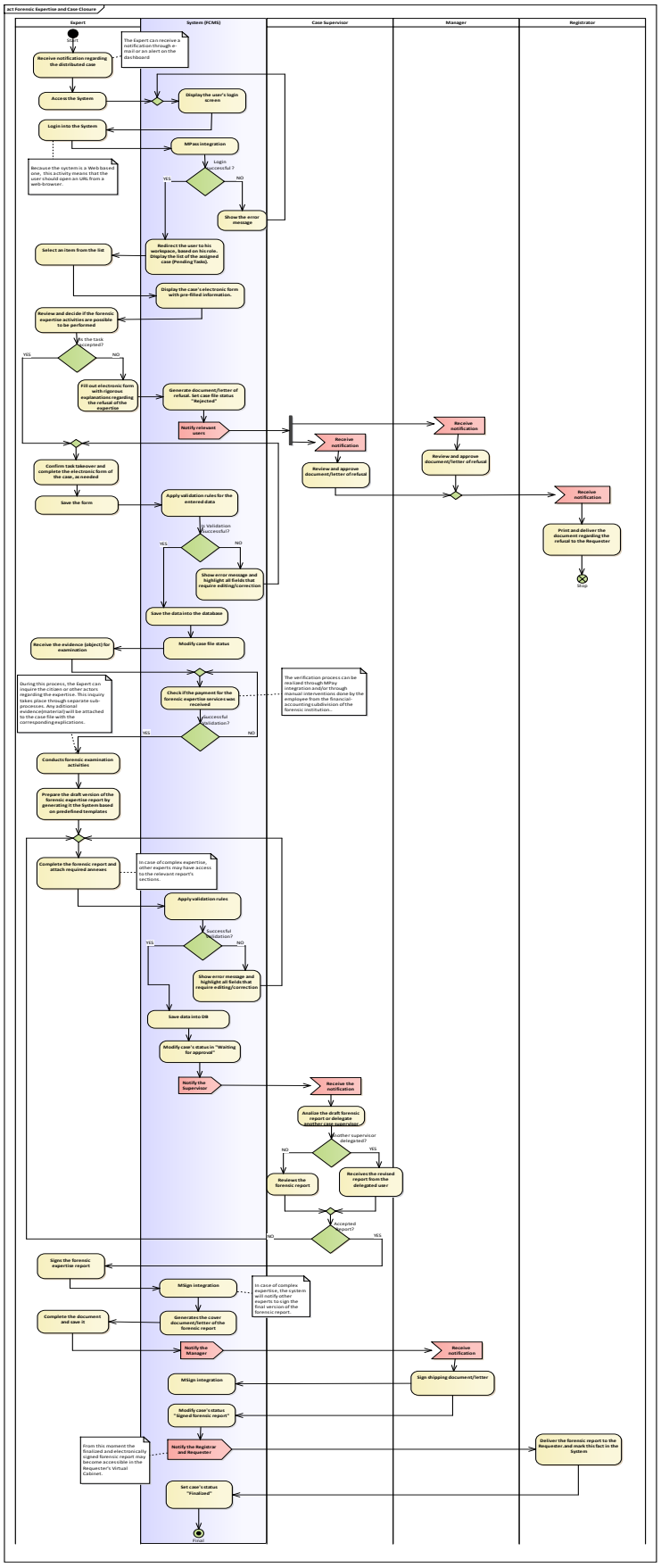


Figure 19. Judicial expertise and finalization of the case

This flow involves forensic examination activities and finalization/closing of the forensic case. The main actor of the scenario is the forensic expert who shall be able to access the list of pending cases, either from the dashboard or from the workspace's main menu. In response, the System shall display the list of new cases assigned to the user.

Further, the Expert will select the case from the list, and the System will display the already pre-filled in electronic form of the case, with the possibility to access the request/application and any other documents or information related to the forensic case.

After a careful review, the Expert shall complete, if necessary, the case's electronic form's section relevant to his/her role and will confirm the takeover of the case. Once the task is accepted by the user, the System will change the status of the case, informing all other involved users.

Considering the legal framework in force, especially Art. 53 of Law no. 68/2016 on forensic examination and the status of the forensic expert, this flow shall contain a decision-making activity, which shall be taken by the Expert. Namely, the expert shall have the possibility (after reviewing the requirements to the forensic examination, capabilities and resources needed to be used) to reject the forensic examination/case which has been assigned. In such a case, the System shall generate the case rejection document/letter, in which the user (Expert) must provide all relevant explanations, as well as the reference to at least one or several criteria according to Art. 53 of Law no. 68/2016. The document must be signed electronically and, if necessary, handwritten in paper format, and subsequently sent to the requester through the Registrar role, but with prior notification and approval of the Case Supervisor and Manager of the forensic institution. The System will assign a unique ID to the document and will attach it to the electronic case. Additionally, the System will automatically set the status of case as 'rejected'. Based on the assigned status, the System will subsequently be able to generate statistical and analytical reports on recorded cases.

Otherwise, if the Expert has confirmed the acceptance to perform the forensic examination, he/she shall initiate the forensic examination activities, and the System change the status of the case "in progress".

It should be noted that other sub-processes may take place within the forensic examination process, which will also be digitized through the FCMS. Some of them are:

Requesting additional clarifications from the Requester. This sub-process involves communication with the requester to obtain additional information about the details of the forensic examination to be applied to the object (evidence). Communication shall take place by generating an outgoing document in the System according to a predetermined template. A unique ID shall be assigned to the document, it will be submitted through the Registrar and will be attached to the electronic forensic case.

Any response received from the Requester or other external actor with reference to the forensic case, will be uploaded into the System as an incoming document through the Registrar role and must be attached to the concerned case, making reference to the previous outgoing document as well.

Dispatching/Receiving the evidence (object of forensic examination). This sub-process involves the documentation/registration in the System of any operation related to the reception or transmission of the object between users/subdivisions or laboratories. This sub-process involves the use of barcode scanners.

Requesting laboratory examinations. In some cases (e.g. forensic medical examination and not only) may involve not only forensic activities on the part of the Expert, but also special laboratory investigations and tests. For example, an Expert may need a specific laboratory investigation to be performed so he must be able to generate the respective request in the System, indicating the responsible laboratory and evidence to be examined. The System will generate and assign a unique ID to the request and will include it in the electronic case. During the laboratory examination process the laboratory experts shall be able to complete the relevant electronic forms related to the examination they carry out. Upon receipt of the response (e.g. the Laboratory Examination Report) from the laboratory, it must be attached to the case and appropriate access will be guaranteed only to relevant users, such as the expert who requested the laboratory research and the head of the subdivision.

The sub-process of requesting laboratory researches includes the following steps:

- accessing the System through the MPass governmental service by the user (expert) of the forensic

institution;
- selecting and accessing the forensic case;
- accessing the feature of requesting laboratory research. In response, the System shall display on the screen the pre-filled form related to the request of a laboratory research;
- filling in all mandatory and, where appropriate, optional fields by the expert, such as the type of investigation requested, the laboratory, the deadline and other relevant data;
- saving the request to perform laboratory research in the System database;
- notification of all relevant users, including the laboratory specialist, of the new request.

The sub-process of processing laboratory research results includes the following steps:

- accessing the System through the MPass government service by the laboratory specialist of the judicial institution;
- selecting and accessing the request for laboratory research;
- accessing the feature regarding the documentation of the laboratory research results. In response, the System will display on the screen the pre-filled form regarding the result of the laboratory research;
- filling in all the mandatory and, as the case may be, the optional fields by the laboratory expert and uploading the laboratory examination report;
- application of the electronic signature of the laboratory specialist, who performed the research;
- saving the registration and the report in the System's database;
- notification of all relevant users, including the expert who requested the laboratory examination.

It should be noted that at any stage of the flow, users will only fill in the relevant fields of the electronic sheet related to the process activity and no more entries will be made in the registers, as they can be generated automatically by the System.

Once the forensic examination has been performed, the Expert can generate from the System the blank form of the judicial expertise report (e.g. forensic report, non-forensic report, technical and scientific fact-finding report, forensic medical fact-finding report) according to a pre-set template depending on the specifics of the forensic institution in which the expert works. He/she will fill in all the relevant sections and will attach any other necessary documents/materials, after which he/she will save it in the System.

Once the report has been saved, the System will change the status of the case and will notify the Case Supervisor of this fact. The Case Supervisor will access the list of pending cases, will select the newly created forensic report and will review it. The Case Supervisor has the option to carry out the review independently or to delegate this task to another user (case supervisor). Regardless of the scenario, the Case Supervisor will indicate this in the System. Subsequently, the Case Supervisor may have two options:

Returning the report to the expert, but by necessarily offering explanations through the feedback/comment tools in the System. In this case, the System shall immediately notify the executor, who shall make any necessary adjustments to the report and return it for acceptance to the Case Supervisor. This cycle will continue until the Case Supervisor validates the report;

Acceptance of the report – assumes that the Case Supervisor accepts the forensic report and marks this fact in the System, by activating the option 'Acceptance of forensic report'.

Once the report has been accepted by the Case Supervisor, the Expert (and other experts as appropriate) will apply the qualified advanced electronic signature on the document (through the MSign service), which will become final and non-editable, read-only. At the same time, the System will generate the cover letter according to a pre-set template.

Once the cover letter has been completed and saved, the System will notify the Manager about the need to sign that document. The case's status will be changed as 'signed forensic report'. It should be noted that the forensic report will be identified with the unique number (Unique ID). Moreover, any document or report generated in/by the System will be assigned a unique identification number (ID) so that they shall not be confused.

The forensic report together accompanied by the cover letter will be submitted to the requester through the Registrar.

All appropriate records regarding the requester's notification, including the date and time, will be recorded in the System. At the same time, the System will notify the requester through the Virtual Cabinet and/or an e-mail message about the completion of the forensic examination and about the need to pick up the evidence (object of the forensic examination), as well as about any other relevant information to the case.

It should be mentioned that, as long as the evidence hasn't been returned to the requester, the forensic report in the Virtual Cabinet will remain unavailable for downloading and the case will not be closed. Once the evidence (objects of the forensic examination) has been returned to the requester, the signed forensic report will become available for download in the requester's Virtual Cabinet and the System will set the case's status as ''finalized.

It is also worth mentioning that once the case is finalized it will be archived (including the forensic report and all other documents, information and data). The System shall deny the access to archived cases, including to the author-expert. Archived cases may be accessed according to a special procedure through the Registrar and subject to the Manager's approval. This kind of actions shall be strictly logged.

In order to perform the archiving functions, the System will comply with at least the followings:

- for all completed forensic cases, which means that the forensic report and the examined evidence have been received by the requester, the archiving process will be triggered automatically by the System;
- all documents and information in the forensic case to be archived will be migrated to the digital archive's database and the access will be denied to any user, including users who participated in the forensic examination.
- the case will acquire the 'archived' status in the System, and its metadata can only participate in the statistical reporting process, without disclosing other information, documents or other type of content of the case.

11.5. Evidence Management (objects subject to forensic examination)

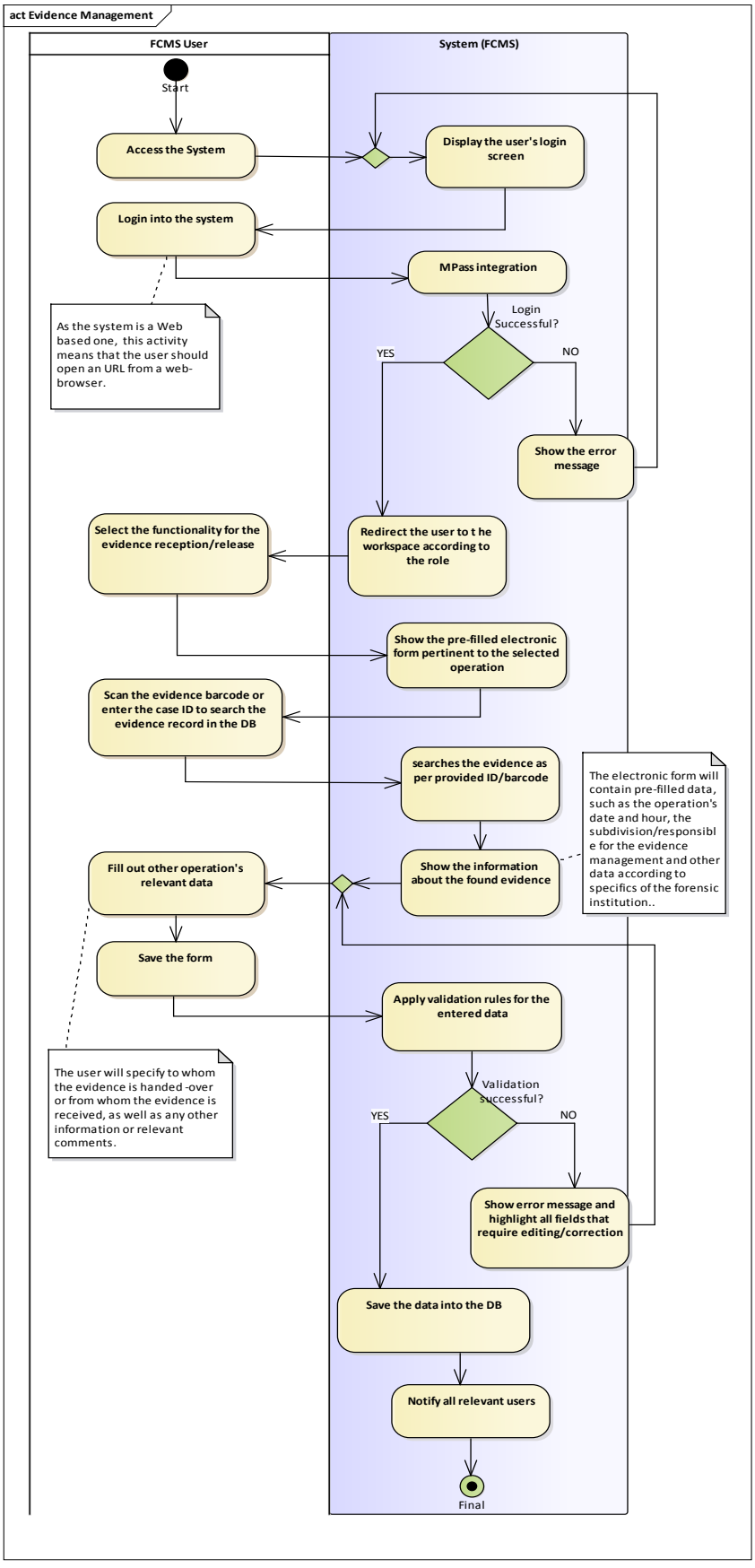


Figure 20. Evidence management

The features related to the registration of receiving/dispatching operations of the evidence may be combined by different roles, including the Case Supervisor and/or the Expert or a special depositary role.

Thus, the flow will start by accessing the FCMS through a web browser and authentication, using the MPass service. If the authentication is successful, the System will redirect the user to the main page, which represents the user's workspace. It will contain at least a dashboard, which displays a short summary of the current state in terms of user's tasks and the main menu.

Further, the user will choose from the main menu the operation of receiving or transmitting the evidence. In response, the System will display the electronic form of the evidence. The user shall scan the barcode using a barcode scanner, and as response the System shall identify the evidence (object) and fill the electronic form of the evidence. Even if the evidence's electronic form is pre-filled by the System, some fields will be editable, so that the user will be able to complete them if so required. The user shall select the subdivision and the employee to whom the evidence is handed-over. Then next user shall confirm the taking-over of the evidence.

Once the data of the electronic form have been entered, the user shall press a 'Save' button and the System will trigger the validation procedure for the entered data. This can involve both Client-Side and Server-Side validation rules and processes. If incorrectly entered data are detected, the System will display the corresponding error message and will highlight the fields to be edited/corrected. Once all data have been entered correctly and validation rules have been successfully applied, the System will save the data into the DB and all relevant users will be notified about the operation.

Any essential operation in the System must be necessarily logged, in particular those related to handling the evidences (objects of the forensic examination). The System will record at least the date and time, the user, the type of operation, the evidence's ID, case's ID and other relevant data.

In order to ensure the correctness of the operations related to receiving and returning of the evidence from/to the Requester, the System will enable the pre-configuration of users that are allowed to such operations (i.e. users who can get in contact with the requester for the purpose of taking over/returning the objects), depending on the specifics of the forensic institution.

11.6. Processing of incoming documents

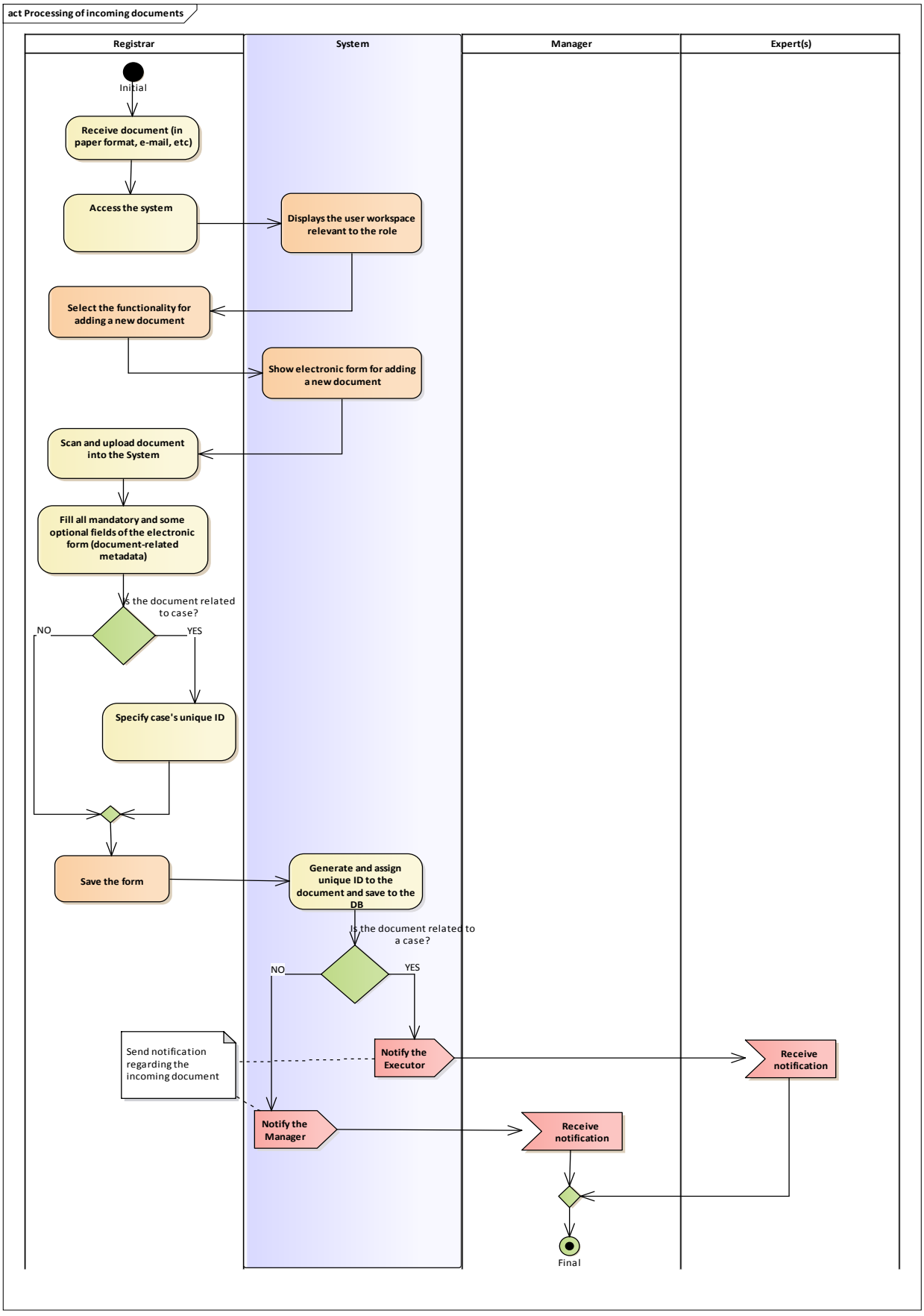


Figure 21. Processing of incoming documents

11.7. Processing of outgoing documents

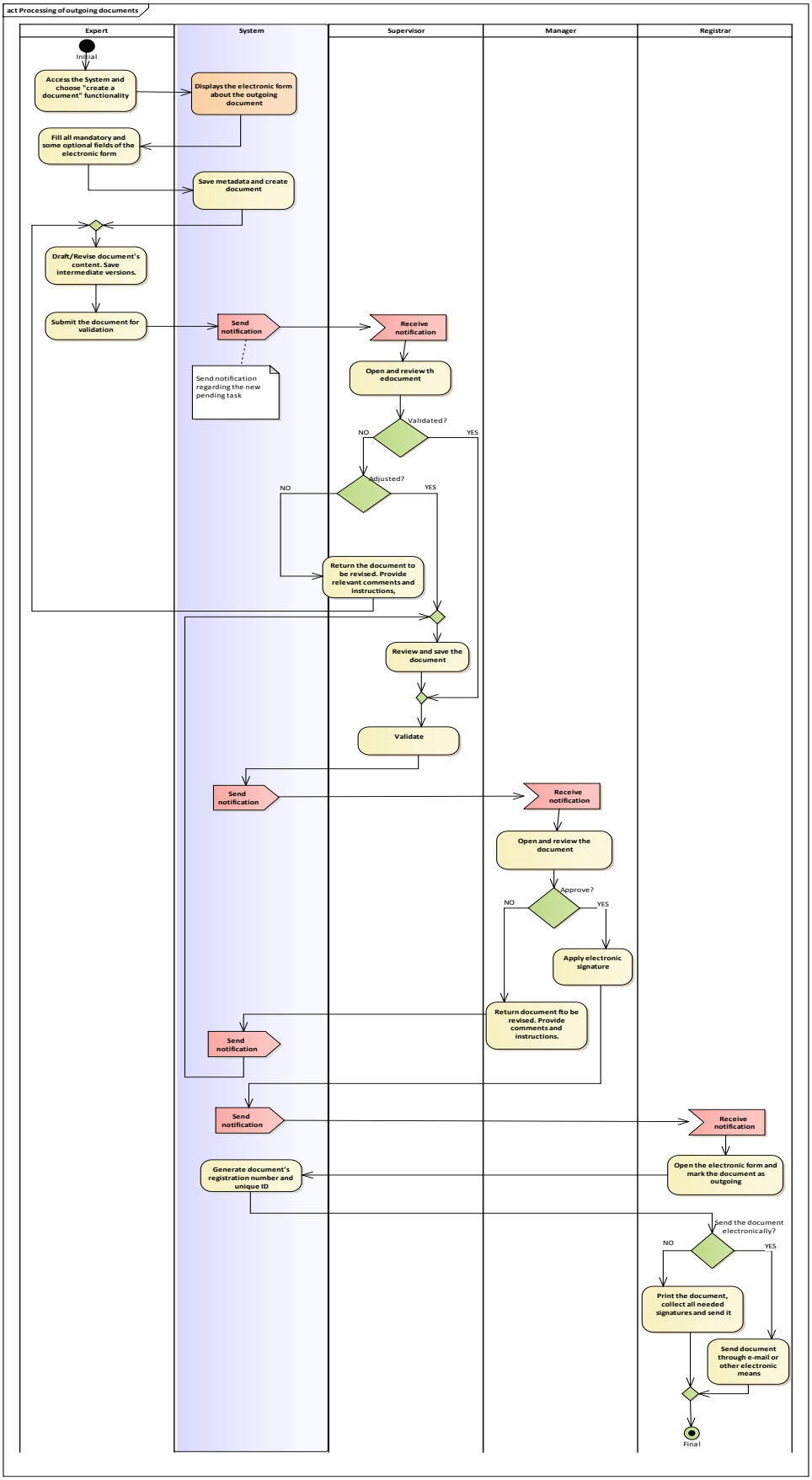


Figure 22. Processing of outgoing documents

12. NON-FUNCTIONAL REQUIREMENTS

12.1. Requirements regarding the System's Architecture

The following general requirements to the System Architecture shall be fulfilled:

Requirement	Type	Explanation
NFRQ001	M	The FCMS solution must be developed based on a minimum 3-levels/layers architecture (i.e. Presentation Layer, Business-logic layer, Data layer), in a way that higher layer interacts only with preceding lower layer.
NFRQ002	M	The Architecture must be open, modular and based on integrated components. These principles must be visible at all levels of the architecture.
NFRQ003	M	The System will optimize processing of queries (i.e. caching of queries).
NFRQ004	M	The System uptime shall be at least 99.5%, with 8 hours Recovery Time Objective (RTO) and zero data loss Recovery Point Objective (RPO).

The Architecture's Presentation Layer enables user interaction with the business functions of the new System. The requirements for the presentation layer are listed below:

Requirement	Type	Explanation
NFRQ005	M	The forensic institution's and other users will use web browser to access all the functionalities and data in the System for which they are authorized. The new System shall support cross-browser compatibility, by means that users shall be able to access the System using standard web browsers using either desktop or mobile devices. In this sense the new System will be compatible with at least 2 most recent versions of the following Web browsers: Microsoft Internet Explorer, Microsoft Edge and Google Chrome.
NFRQ006	HD	The System shall implement HTML 5 web interface and should use only web browser. However, in case of certain specific functionality, the System may use certain minimum supplementary installations (e.g. web browser add-ons) if needed. This remain at the decision of the software development team and MJ. The graphical user interface shall be in Romanian language.
NFRQ007	M	The presentation layer won't implement any business rules, except of the validation of data entry.

Requirement	Type	Explanation
NFRQ008	M	The new System must be accessible by any user authorised by the Beneficiary which is connected to the Internet using standard devices (e.g. desktop stations, portable computers and other suitable mobile devices). For this purpose, the GUI must have a respective design.

The Business Logic Layer of the new System's Architecture shall implement at least the functionalities, as per Chapter 6. 'Functional Requirements' from this document. This layer is responsible for accessing, processing and transformation of the data. It manages the business rules and assures the data consistency and accuracy. The business logic layer is accessed from the presentation layer to make the functionalities available to the users and it can also offer the functionalities to external information systems through the data exchange interfaces.

The requirements for the business-logic layer are defined as follows:

Requirement	Type	Explanation
NFRQ009	M	The Business Logic Layer must be completely independent from the Presentation Layer and from other external applications that use the data exchange mechanisms.
NFRQ010	M	The Business Logic Layer must have a completely modular architecture based on reusable components and abstract interfaces. There must be no identical functions made by different components (e.g. data access).
NFRQ011	M	The Business Logic Layer must contain and delimit the "business-processes workflow" and "business entity" components.
NFRQ012	M	Access to business entity components will be done through business workflow components.
NFRQ013	M	The business entities must be clearly defined at the Business Logic level.
NFRQ014	M	Business entity components must contain all data and business logic related to the business entity, for undertaking the business operations, implementation of relevant business rules and for the maintenance of the integrity and accuracy of contained data.
NFRQ015	M	The components related to Business Logic Layer must communicate through dedicated interfaces/ internal functions (tight coupling).
NFRQ016	M	The components of the Business Logic Layer may be accessible for external applications only through the data exchange interfaces.
NFRQ009	M	The architecture of the Business Logic Layer will allow simultaneous

Requirement	Type	Explanation
		access to the functionalities of the System.
NFRQ010	M	The components of the Business Logic Layer must be developed in modern and widely used programming language(s) while developing web applications (e.g. C#, Java, etc.). The exact list of the programming languages remains at the decision of the software development team.
NFRQ011	M	The technology at this layer must allow seamless integration of the functional modules of the System.

The new IT System database(s) and data will be implemented using the relational database management System (DBMS). The requirements for the Architecture's Data Layer are defined as follows:

Requirement	Type	Explanation
NFRQ012	M	The data model implemented at the Data Layer of the System must follow at least the third-normal form for the database design, to reduce the duplication of data and ensure referential integrity.
NFRQ013	M	The System data model must follow the Common Data Modelling with a generic Data Model which consists of generic types of entity like class, relationships, and others.
NFRQ014	M	The data at the Data Layer must be accessed only through the Business Logic Layer and independent from the Business Logic Layer.
NFRQ015	M	The data model must be updated/completed by the contractor's team, it must contain both the technical description of the data (e.g. entity-relationship diagrams, structures of databases, objects in databases, etc.), and the semantic description (association of data structures with business entities and their properties). The semantic description has to be available for users, where applicable (e.g. customization of reports).
NFRQ016	M	The Data Layer must assure the integrity and accuracy of data (transaction integrity).
NFRQ017	M	The Data Layer of the System's Architecture shall support relational database management systems that have at least the following modern capabilities: • Effective utilization of RAN and SIMD instructions; • Columnar format for tables (including encoding); • Partitioning; • Virtualization, deployment.

Requirement	Type	Explanation
NFRQ018	M	The System will be implemented using a single database management platform implemented in high-availability (e.g. failover cluster, mirroring).
NFRQ019	M	The System's DBMS will provide at least the following general features: • Be able to identify and resolve deadlock situations; • It shall allow primary key and foreign key constraints; • It shall allow fields to accept NULL values; • It shall provide the ability to impose constraints on data types and values, if so needed.

12.2. Requirements regarding the Technologies

At this level there are the software and hardware components needed for the running of the System (Presentation Layer, Business Logic Layer, Data Layer).

The Contractor is responsible to include in its offer all needed software at this level for well-functioning of the offered software solution and to define the deployment model of the System in the MCloud.

The requirements regarding architecture for the technological level are presented in the following table:

Requirement	Type	Explanation
NFRQ020	M	The technology architecture must have a high level of resistance to failure and must not contain single points of failure (SPOF).
NFRQ021	M	The technology architecture must assure rational and balanced use of processing resources.
NFRQ022	M	The technological platform shall be made up of the totality of software and hardware components needed to assure the operating environment for the System. Regarding hardware, the Contractor must provide the requirements for virtual machines, as the System will be hosted in the MCloud. The technological platform for software includes: software development platforms, database management system, operating systems, and any other software including third-party software needed for the System to operate. The Contractor must provide all software for the offered solution to operate.
NFRQ023	M	The Contractor is responsible for implementation and configuration of the software to the designed hosting environment in the MCloud.
NFRQ024	M	The technological platform for software must be widely used in several countries, and must be locally supported in Republic of

Requirement	Type	Explanation
		Moldova by a partner who is authorized by the manufacturer.
NFRQ025	M	The technological platform for software must be independent from the hardware technological platform (i.e. it shall run on at least two types of processors from different manufacturers).
NFRQ026	M	The technological platform for software must be homogeneous. This means that it must consists of minimal number of different technologies, e.g. same operating systems for middleware and database).
NFRQ027	M	The technological platform for software must support the creation, modification, processing, storage and accessing of textual data in Unicode format.
NFRQ028	M	All components of the System (e.g. middleware, databases) shall run on platform with operating systems from the Windows Server or Linux family which are supported in the governmental cloud infrastructure "MCloud". The supported versions of the operating systems must be maintained by producers and shall belong to the latest 2 major versions.
NFRQ029	M	For running of the System at the client side, the Contractor shall specify the needed equipment which can be purchased from the local market in Moldova.

12.3. Security Requirements

General Technical Requirements Related to the System's Security

The new IT System shall implement at least the following requirements in terms of Security issues:

Requirement	Type	Explanation
NFRQ030	M	The System has to support the following informational security requirements according to the Information Security Standard: • Information integrity – maintaining and assuring the accuracy and completeness of data over its entire life-cycle; • Confidentiality – protection from unauthorized access to data; and • Availability – to ensure the availability of the information when needed.
NFRQ031	M	The System has to support the following main mechanisms for

Requirement	Type	Explanation
		ensuring the informational security: • Authentication and Authorization; • Managing access to information; • Recording actions of users in the System and transactional logs; • Encryption of information, where needed; • IT audit; and • Business-continuity and disaster-recovery.
NFRQ032	M	The Architecture of the new System is conceived using a secure by design approach.
NFRQ033	M	The security architecture of the new System shall be documented at the detailed technical level by the software development team.
NFRQ034	M	All System processes associated will work with minimum privileges required to perform assigned tasks.
NFRQ035	M	The new System shall allow creation of User Accounts and User Roles. The System will provide reporting services for user activities and allow allocation and management of users' access rights (create, read, update and delete).
NFRQ036	M	All access credentials used by the System must be configured in the administrative interfaces. The System MUST NOT contain hard-coded access credentials.
NFRQ037	M	The System must support users access based on secure passwords (mandatory) and other types of access (Active Directory-desirable).
NFRQ038	M	The System shall guarantee the full protection and integrity of the database content.
NFRQ039	M	The access to features offered to users outside forensic institutions offices will be controlled by overload protection of the service by one or more network nodes.
NFRQ040	M	All fields filled in by users must be validated according to the type of client and server.
NFRQ041	M	The System must support encrypted communication channels, such as HTTPS, SSL and TLS, if so needed. This shall be decided during the software development phase by the Contractor.

Requirement	Type	Explanation
NFRQ042	M	The new System MUST ensure the confidentiality of the data transmitted through the communication channels.
NFRQ043	M	The users' actions shall be recorded in electronic logs.
NFRQ044	M	The System might emit a periodic signal indicating its functional status.
NFRQ045	M	The System shall support standard security features such as automatic disconnection after a period of idle status (e.g. 10 min). This parameter shall be configurable for the web application.
NFRQ046	M	The System shall allow the temporary blocking of the user's access in case of multiple failed login attempts.
NFRQ047	M	The System must support the critical information access blocking even for the System administrators.
NFRQ048	M	Only authorized ITCSS personnel – System administrators shall have access to logs of operations.
NFRQ049	M	The new System shall guarantee the protection of the stored data by ensuring that the core data cannot be accessed without log-in through the provided User-Interface.

12.4. Requirements to the User Authentication Mechanism

Additionally, to the above-mentioned requirements, the new System shall implement at least the following requirements in terms of User Authentication mechanism:

Requirement	Type	Explanation
NFRQ050	M	The System will allow access to its functionalities only after a successful identification of the user / administrator.
NFRQ051	M	For all users from the forensic institutions, the System will use MPass for authentication and authorization purposes.
NFRQ052	M	For the extrarenal users (requestors/applicants) the System may support at least the following authentication methods: based on ID/Username and password.

Requirement	Type	Explanation
NFRQ053	M	The System will allow external users to change their individual passwords.
NFRQ054	M	The System will allow external users to register their account information (example: ID, password, name, surname, email, etc.).
NFRQ055	M	The users' passwords must be protected. The method of protecting passwords must ensure that they are not intercepted, seized or recovered.
NFRQ056	M	The new System will enable defining and implementing a set of rules for using passwords, in case of external users. The policies must allow conditions to be set at least for: • complexity of password • mandatory password change • term of validity of the password • re-use of passwords • the number of failed authentication attempts allowed • a dictionary of forbidden passwords, if so needed.
NFRQ057	M	The System will provide the external user with timely information on the application of policies for using the passwords.
NFRQ058	M	The System will allow differentiated use of policies for using passwords for different user groups.
NFRQ059	M	The System will allow external users accounts to be disabled or suspended at the application level.
NFRQ060	M	The System will allow setting the expiration time for user sessions in case of inactivity.
NFRQ061	M	The System will have effective mechanisms to prevent the unauthorized download of active sessions initiated by legitimate users.
NFRQ062	M	A System's work session will be blocked at the request of the user or automatically at the end of the user's session.

12.5. Requirements to the User Authorization Mechanism

Additionally, to the above-mentioned requirements, the new System shall implement at least the following requirements in terms of User Authorization mechanism:

Requirement	Type	Explanation
NFRQ063	M	The System will allow granular management of access rights to all objects of the information system and possible actions (e.g. screens, buttons, menus, menu options).
NFRQ064	M	The System will allow the definition of user groups and roles within the system and assigning users and groups to these roles.
NFRQ065	M	The System will allow the granting of access rights to the user explicitly, group and role. A user can be assigned one role, its rights of access can be determined on a cumulative basis.
NFRQ066	M	Access to data within the System shall be controlled by security parameters.
NFRQ067	M	The new System will have appropriate mechanisms for protecting data entry (incoming data from authorized users, input from external sources).
NFRQ068	M	All actions for changing data within the System will be made through specialized GUI forms in accordance with the business-process workflow. Under no circumstances, the end user can have access to make changes at the level of DB.
NFRQ069	M	The System will have additional mechanisms for protecting privacy data according to the Moldovan Data Protection legal framework.
NFRQ070	M	The new solution will have appropriate mechanisms to prevent the unauthorized manipulation of data that are stored by the System.

12.6. Requirements for Managing Exceptions and Errors

This section sets out the requirements for the mechanism for managing exceptions and errors within the new System to be implemented:

Requirement	Type	Explanation
NFRQ071	M	The System will intercept and handle all exceptions and errors generated by its components. All events will be recorded centrally.
NFRQ072	M	When an error occurs, the System must display a generic error message to the user. The form of error messages is dependent on the user type. It may contain an error code and a unique identifier of the error to facilitate support.
NFRQ073	M	The System will use standard tools for analysing and processing the records of exceptions and errors.
NFRQ074	M	If a dependent System's component detects an error, the cause of the error must be communicated to the caller component. Any error should be logged for Administrators' inspection.
NFRQ075	M	Error management must provide comprehensive instructions for identifying of the problem and handling of the error.

12.7. Requirements regarding Usability

The System's interfaces for end-users should be intuitive and easy to use, without requiring extensive technical assistance, support or offline user guides. For System Administrators, guides may be needed to explore advanced

functionalities, but such advanced functionalities should be as intuitive as possible.

Requirement	Type	Explanation
NFRQ076	M	The System shall display friendly error messages to the users. It shall not display to the end users the technical details of the error. The form and content of the error message shall be decided more exactly at the Analysis and Design stage and it will depend on the users' types.
NFRQ077	M	The new System shall follow the simple principle, which involves for each individual System's screen means that two things should be obvious to the end user: Where am I now? and How can I go back? This means these controls have to be close to the top of the screen.
NFRQ078	M	The software development team will make sure the browser's 'Back' button works in a predictable manner in all situations.
NFRQ079	M	System's Maintenance in terms of user interface configuration, user rights management, and data source settings should be done with visual tools.

12.8. Requirements regarding System's Flexibility

The adaptability and flexibility terms refer to the ability for the software solution to adapt to possible or future changes in its requirements.

Requirement	Type	Explanation
NFRQ080	M	The System's Architecture shall be in line with the needs of the forensic institutions in terms of the flexibility and adaptability of the new ICT System. MJ advocates a modular architecture based on independent components accessing the data. These principles shall be visible at all levels of the System's architecture. Therefore, in order for the System to be accommodated, flexible and easy to maintain, there must be used unified technology platform for all processes realized by the System components.
NFRQ081	M	The architecture of the new IT System's shall be able to adapt to the changes in users' environment (forensic institutions) and usability requirements without encompassing structural changes and permitting evolution and growth.
NFRQ082	M	Therefore, the new System shall be at maximum possible a highly configurable software solution, which would enable adjustments of the implemented functionalities with minimum coding effort, by using the administrative/management console.

12.9. Requirements regarding System's Scalability

When using the new System, the number of processed transactions and competing users may be able to be increased or reduced from one period to another. For rational use of processing resources, the new System must be scalable (up and down).

Therefore, at least the following technical requirements related to the new System and its DBMS shall be taken into account by the software development team during the development and implementation:

Requirement	Type	Explanation
NFRQ083	M	The System will provide increased processing capacity without interrupting operations. To this end, the System will support the horizontal expansion of the processing capacity (for example, adding new application servers and load balancing, allocating more resources to the database servers).
NFRQ084	M	The new System can be configured to automatically adjust to key levels (lag-sensitive). The System will be adjusted up and down.
NFRQ085	M	The System must be capable of serving the maximal number of transactions with adequate allocation of resources for data processing and storage. The resources will be allocated in the virtual environment and could be new servers or new resources to the existing servers.
NFRQ086	M	The System must be scalable, which means that it must be able to expand the number of users, with no change in the initial solution. The solution should be scalable both vertically and horizontally. The Contractor shall specify information on possible vertical and horizontal scaling.
NFRQ087	M	The System must ensure a balanced distribution of load on different hardware and software components to operate the System within acceptable parameters with an increasing System load.
NFRQ088	M	The System shall use the functionalities for clustering available in the virtual environment to improve the scalability and business continuity of the System.
NFRQ089	M	The System's DBMS shall support table and index partitioning. The data of partitioned tables and indexes may be divided into units that can be spread across more than one filegroup in a database.
NFRQ090	M	The System's DBMS shall allow the definition of the minimum amount of data transferred between the disk and the local memory of the database upon request.

Requirement	Type	Explanation
NFRQ091	M	The System's DBMS shall allow setting of memory options such as minimum server memory and max server memory, to reconfigure the amount of memory that is managed by the DBMS, which is being used by an instance of the DB Server.
NFRQ092	M	The System's DBMS shall provide the possibility of logical partitioning of large tables in order to reduce the time of access to data according to various partitioning criteria (list, range, hash) and all combinations thereof (range-list, range-hash, etc.). In other words, the database table partitioning shall allow dividing a large table into smaller, more manageable parts without having to create separate tables for each part. Data in a partitioned table shall be physically stored in groups of rows called 'partitions' and each partition shall be able to be accessed and maintained separately. Therefore, the DBMS may allow the System administrators to be able to speed up loading and archiving of data and to perform maintenance operations on individual partitions instead of the whole table. They may be also able to improve query performance.

12.10. Requirements regarding Maintainability

Requirement	Type	Explanation
NFRQ093	M	The number of software (in terms of technological stack) providers for the system's components which are part of the offered solution shall be not more than 2 providers;
NFRQ094	M	The number of development environments used for the development of applications which are part of the offered solution shall be not more than 2;
NFRQ095	M	The architecture of the proposed System shall allow the implementation of changes in a simple way at application level. The boundary affected by changes shall be minimal and the components needed to be tested in the result of changes, clearly identifiable.
NFRQ096	M	The technology(ies) on which the proposed solution will be built shall not be an outdated one. Therefore, the contractor shall build the System on the latest version of the technological platform which has been chosen for its software solution.

12.11. Requirements regarding Resistance and Breakdowns

Requirement	Type	Explanation
NFRQ097	M	The proposed system must have instruments implemented for the execution of backup copying procedures and management of historical backup copies.
NFRQ098	M	The proposed system must have mechanisms of assurance of data integrity in case of breakdown of any components.
NFRQ099	M	The proposed system must have mechanisms of operative restoration of availability and accessibility of applications in case of continuity incidents.
NFRQ100	M	The architecture of the proposed system must be resistant to breakdown of components and must not have single breakdown points (SPOF).

12.12. Requirements regarding System's Performance

Requirement	Type	Explanation
NFRQ101	M	The simultaneous running of internal processes of the FCMS must not have impact on the general performance of the System. Otherwise, the Bidder shall include in the guidelines of the system administration and operation of applications the information regarding the processes that can affect the performance of applications and his recommendations regarding the simultaneous running of these processes.
NFRQ102	M	The average server reply time shall not exceed 3 seconds at nominal system load. However, this is not related to report generation.
NFRQ103	M	The architecture of the System (except requestor's "Virtual Cabinet" component) proposed by the Bidder must assure the following minimum levels of performance for: • Management of a number of 300 accounts of users; • Management of up to 300 simultaneous user connections. This number includes only users from the forensic institutions. The requesters are not included; • The response time to a transactional request user / external service must not exceed three seconds (note: it does not refer to generation of reports).
NFRQ104	M	Performance testing will include minimum two components: system load testing and system stress testing.
NFRQ105	M	The Requester's Virtual Cabinet (public portal) component designed for the external users (applicants and public internet users) must allow an unlimited number of users.
NFRQ106		The generation of reports and the access of information must not affect the operational performance of the System at the level of processing the transactions. Otherwise, in the system's documentation, the reports with significant impact on performance shall be identified and the recommendations of the selected Bidder shall be formulated regarding the generation of reports so that they do not affect the performance characteristic of the applications.
NFRQ107		The FCMS solution must be capable to store all the transactional and historical data for a period of minimum 5 years, without being affected its performance.
NFRQ108		The Bidder Bidder shall indicate in his offer the minimum values secured for the performance characteristics of the applications, taking into account the technological platform recommended by

Requirement	Type	Explanation
		the Bidder Bidder .

12.13. Requirements regarding Interoperability

In order to support the business processes of the involved forensic institutions, the Contractor shall make all efforts as required so that the FCMS to be integrated with other relevant IT systems and e-governance services. The interoperability of the proposed System represents characteristic of communication with other external ICT Systems, applications or services.

The Bidder Bidder /the Contractor shall provide his clear statement and methodology in the technical proposal on how he intends to implement this aspect.

The requirements regarding the interoperability characteristics of FCMS are:

Requirement	Type	Explanation
NFRQ109	M	All the interfaces of the System must be based on open standards.
NFRQ110	HD	The interfaces of the provided System may interact with external applications both in real time and in off-line regime.
NFRQ111	M	The interfaces of the provided System will allow the weak coupling with external ICT systems and services (communication based on messages).
NFRQ112	M	The System shall provide standard interfaces for accessing of all its key business-functions (e.g. generation of documents, generation of reports, accessing the information about the business entities).
NFRQ113	M	All System's interfaces must be properly documented (e.g. by using Web Services Description Language – WSDL).
NFRQ114	M	The proposed FCMS shall have the possibility of creating email messages according to preconfigured templates and sending them to the indicated recipients through an electronic mail server set up in the configurations of the System.

12.14. Requirements to the Dedicated Audit for Applications and Database Servers

Requirement	Type	Explanation
NFRQ115	M	The proposed solution shall be able to be used as separate platform, providing additional operational functions: • engine for collection of events in real time in an operational database; • management tools for the audit database; • the operational database has the purpose to keep data online for 6 months, without having a major impact on the database server; • a separate client interface which can be used by the administrators of the directory service; • the client interface will include all the tools needed for the administration of the product; • the client interface will include a predefined set of reports and filters for investigational purpose.
NFRQ116	M	The proposed solution must extend the native audit capacities at level of transactional log, both at level of application server and database server, with the purpose of capturing any critical changes or the activity of user and/or administrator in detail, in view of immediate detection of actions and the recognition of their significance; must highlight who, what, when, where and from what station made a change.
NFRQ117	M	The proposed solution must allow granularization in the smallest detail e.g.: • SQL broker auditing (or similar), database, object, performance, SQL roles and transaction events as well as errors and warnings; • Auditing of users' actions in real time; • Completion of functions of detection and prevention of intrusions by a permanent monitoring of actions inside the databases.
NFRQ118	M	The proposed solution must not be based on native audit logs, which are difficult to activate and manage, whose activation implies the significant additional loading of application servers and database servers.
NFRQ119	M	To assure full flexibility, the security administrators must be able to configure the System granularly so that certain categories of events are recorded exclusively in this events' log, in order not to load from operational point of view the client administrative interface.

Requirement	Type	Explanation
NFRQ120	M	The solution must provide a predefined set of intelligent alerts, in real time, when critical objects are modified or when certain patterns of changes are detected.
NFRQ121	M	The proposed solution must provide a management of changes at the level of all involved forensic institutions from a unique client and allow the storage of all audit data in a single centralized and secured database.
NFRQ122	M	The proposed solution must reduce the resolution times of problems by grouping, sorting and filtering the search results by type of events, user account, objects etc.
NFRQ123	M	The proposed solution must include preconfigured and customizable reports for fulfilling of the audit requirements.
NFRQ124	M	The proposed solution must allow the generation of intelligent alerts which allow the correlation of audited events.
NFRQ125	M	The proposed solution must provide reports switchboard type for all the data audited or for specific data without requiring knowledge of architecture or administration.

12.15. Audit and Control

The following requirements related to audit and controls shall be taken into account during the development and deployment of the new System:

The Contractor's software development team shall keep a System development version in the Development Environment at any time.

At least 70% of the developed specific System components shall be subject to internal unit testing. This is not applicable in case of using third party products.

The software development team shall maintain the components of the development environment and support the versioning of the developed and installed components.

The Contractor's software development team shall document and address the Beneficiary's requests that will be classified into defects and modification requests, if appropriate.

The Contractor's team shall install the System components according to the installation guidelines, which is a deliverable to be submitted to the MJ and ITCSS' technical staff. Also, the Contractor's team shall install the System components together with the ITCSS' System Administrator.

The software development team shall modify the configuration parameters according to the installation guidelines, if

so needed. This must be done in presence and together with the System administrator.

The system administrators shall manage, monitor, and analyse the overall health of the system. In this sense the new System shall provide features for collecting information related to the overall health of the system

13. OTHER PROJECT-RELATED ASPECTS

13.1. Hardware Specification

This project does not include procurement of any hardware for hosting of the System to be developed/implemented. The proposed IT solution is planned to be hosted in the governmental cloud infrastructure "MCloud" which is being managed by the Electronic Governance Agency and technically by the ITCSS. Both institutions are subordinated to the State Chancellery of the Republic of Moldova.

The Contractor will have to specify in his technical proposal the detailed specification of the hardware resources needed for the functioning of the proposed IT solution. Also, the Contractor shall provide detailed specification of needed end-users' hardware, if any (e.g. PCs, scanners, etc.).

13.2. Requirements regarding Software Products and Licensing

The proposed FCMS solution and any related software must be fully covered with licenses (if so required) according to the manufacturer licensing policy which will be granted to the Beneficiary of the System). The Contractor shall deliver perpetual licenses to the Beneficiary that allow FCMS users to use the software for as long as the Beneficiary complies with all terms of the license agreement. There must be no additional or hidden licensing costs for the proposed FCMS solution. All needed licenses for any software used in FCMS shall be provided by the Contractor, included in the Total Price and reflected in the Financial Proposal.

In the case an open-source System is proposed, a commercial subscription that includes patches, fixes and configuration for at least 3 years must be included in the offer.

The Contractor must deliver a "*turnkey*" solution, including project management, preparation and coordination of the proposed appliance architecture and software development, customization, installation, acceptance tests and professional assistance during the production startup. The offer must include detailed description of the proposed services.

The Contractor must obtain all necessary copyright and other Intellectual Property Right permissions before making any Third-Party Material available as Auxiliary Material for the purpose of the implementation of the System.

As the proposed System will be hosted in the MCloud, the Contractor must take into account the fact that in the MCloud the following software is available, for which the Contractor shall not include the costs for licenses:

- OS: Microsoft Windows Server; and
- Linux-based OS.

All software products used for the proposed software solution must be covered with customer support, with SLA 8x5 for at least first 12 months, starting from the date of acceptance of the System.

The Contractor must provide official authorization letter from the manufacturer for reselling the license.

13.3. Intellectual Property Rights (IPR)

All Intellectual Property Rights in the Contract Material vests in UNDP, which may subsequently handover the System and the IPR to the Beneficiary.

The Contractor retains all Intellectual Property Rights in: (a) any COTS Software and existing derivatives thereof and (b) any other of Contractor's Pre-existing Intellectual Property, which Contractor shall furnish during the course of the System implementation through a License.

If the Beneficiary needs to use any of the Auxiliary Material owned by the Contractor or any other of Contractor 's Pre-existing Intellectual Property to receive the full benefit of the Services, the Contractor shall grant a license to the

Beneficiary. The Contractor shall provide perpetual and unlimited user licenses to the Beneficiary

If the Contractor needs to use any Material owned by the Beneficiary or any Contract Material as defined for the purpose of performing its obligations to implement the System, the Beneficiary will grant to the Contractor, royalty-free, non-exclusive, non-transferable license to use, reproduce, adapt, modify and communicate such Material solely for the purpose of providing the Services and Deliverables.

The UNDP and the Beneficiary of the System will have the right to use the FCMS software required for an indefinite period, according to these ToR. The Beneficiary will not have the right to sell the FCMS software to third parties. The software platform will remain the intellectual property of UNDP and the Beneficiary, who is entitled to develop, equip and adapt it as a product or service.

All data stored in the FCMS databases are owned by the relevant Moldovan state bodies. Access to these data is subject to the terms and conditions regarding the confidentiality of the information throughout the entire contractual period of the Contractor and beyond.

The Bidder will submit its proposed license model for the FCMS solution, which will satisfy the aforementioned requirements. The Bidder will describe the proposed licensing and IPR models and provide arguments on why this is best model for this project.

13.4. Management of the Source-Code

The Contractor shall provide the successfully compiled and documented source code (including third instruments and libraries, where applicable).

The Contractor should use a tool similar to GitHub (https://github.com) to manage all versions of software applications that will be iterated across the software development lifecycle, as per agreed Development Plan.

All project documents related to the software development phase should also be uploaded and maintained in GitHub-like tool.

All members of the software development team, as well the UNDP or MJ's responsible project supervisor need to have a registered user account with the aforementioned tool (e.g. GitHub) in order to access all files.

Under no circumstances shall any external persons have access to any uploaded file. Access to all files stored in GitHub shall be restricted to members of the software development team and aforementioned project supervisor.

13.5. Requirements regarding provision of Services

The services of support and post-implementation maintenance during Defects Liability Period/ Warranty Period shall be provided by the Contractor and shall assure the removal of incidents and problems which occurred in the use of the System, which will be addressed and solved in due course, with minimum impact on the activity of the users.

The Bidder has to describe in the technical proposal the activities which will be carried out in order to meet these requirements. The Bidder has to present the way in which he intends to provide the services required by this ToR and his technical, organizational capacities and competences which confirm the Bidder's capacity to execute such a contract.

As part of the initial agreement for the delivery and implementation of the System, the Bidder will provide a post-implementation warranty, which implies the provision of support services and maintenance services for the applications provided, for a period of 12 months from the date of final acceptance of the System.

The price for the warranty services included in the initial agreement shall include all the support and post-implementation maintenance services.

After the expiry of the warranty period the owner of the System may request the extension of services provision based on the cost specified in the Price Schedules under Installation and Other Services. The Bidder shall accept the subsequent provision of services for the period required by the owner of the System.

The support services in the warranty and post-implementation period will be provided by the Contractor, regardless of causes that led to the occurrence of the incident (e.g. errors in application, problems at level of

third-party software).

For this purpose, depending on the specificity of each incident case, the Contractor shall include but not limit to the following activities:

- Reception and recording all information and complaints about the incident produced and the context from the Beneficiary;
- Localization of the incident and identification of immediate activities which must be carried out to reduce the impact of the problem or incident;
- Identification of the causes of the incident and establishment of the actions needed to be carried out to remove the incident;
- Guidance of the Beneficiary in view of performing actions for the reduction of the impact of the incident and its resolution in the time limit established;
- Presentation of detailed information to the owner of the System regarding the causes of the incident, reasoning of actions carried out and planned actions to prevent the repetition of similar incidents.
- Examination of the need for registration of a new problem in relation to the System. In case of the problem registration, the selected Contractor will manage it according to the requirements for the support services for problem resolution.

Requirements regarding Maintenance Services

The maintenance services to be provided by the Contractor for maintaining the normal operation of the System. For this purpose, the Contractor shall provide updates and changes in the System without additional costs during the post-implementation period. The owner of the System may request 3-5 days of the training for staff to be updated about changes introduced in the update of the System without additional costs.

Level of provision of support services

The Level (performance criteria's) of provision of support services is determined by parameters these services must be provided by the Contractor. The Contractor shall describe in his offer the methodology how needed/requested support services will be provided (location of the certified support center, mobile support center, etc.).

The parameters which characterize the level of support services are:

- Response Time (TR) – is the time in which the selected Contractor will react to a support request, will diagnose the situation and will establish the actions that must be carried out for resolution.
- Resolution Time (TS) – is the objective time in which it is expected that the selected Contractor will

carry out the actions in his area of responsibility for the complete resolution of the client's request.

The classification of severity of incidents is identified in the following table.

Table 2.1 Classification of incidents

Classification	Impact on the quality parameters for the operation of applications
Critical	The application is unavailable for all or the majority of business users. The important transactions need to be made as soon as possible (in hours).
High	The application is unavailable for good part of users. Important transactions and operations need to be made until the beginning of the next day.
Ordinary	The application is unavailable for part of users. There are transactions and operations that need to be made in the next three days.
Low	The application is unavailable for a limited number of users. There are no transactions and operations to be made in the next three days.

The Contractor shall be able to provide support services in the working days in accordance with the legislation of the Republic of Moldova, between 09:00 – 17:00.

13.6. Training of Users

13.6.1. The Contractor's team must prepare the detailed training programme, including the training materials for training of the target groups.

13.6.2. The programme and training materials shall be approved by the Beneficiary before commencement of the training. Training materials used during training sessions shall be prepared in Romanian, printed and filed.

13.6.3. In addition, one set of the documents should be presented on CD or memory stick.

13.6.4. The backstopping team shall prepare, print and deliver training materials in form of manuals for each target group, persons attended to the training. Format and number of the copies shall be coordinated with MJ and forensic institutions.

13.6.5. The curricula for the IT technical staff group will cover the entire set of components and controls used for the configuration of the new System. A final exam shall be conducted after the trainees will implement an individual task of configuration of the System (simple but covering main components and functions).

13.6.6. MJ has the right to make changes in the training programme and request additional trainings in case of unsatisfactory performance.

13.6.7. The software development team will provide ToT (training of trainers) training to the key-users

appointed by the MJ and national forensic institutions, considered as target group, aimed to deliver skills in future maintenance of the newly provided solution. Along with the curriculum, training materials will be developed, including relevant System maintenance questions.

13.6.8. The training materials for end-users – shall contain but not limited to a detailed explanation of the use of the System; detailed responsibilities of each user role, system's functionalities and other appropriate information. Training of the users' trainers must be conducted in Romanian language. The training materials shall be provided in Romanian language.

13.6.9. The Contractor shall create a video-tutorial as supporting instruction for the users in Romanian language.

13.7. Deliverables

List of Deliverables

Identifier	Description / Explanation	Estimated Deadline
1	Inception Report and Preliminary Project Plan	During the first week after signing of the contract
2	Detailed SRS (System Requirements Specification) + SDS (System Design Specification including UI/UX) and detailed technical requirements for the needed servers and other hardware infrastructure; technical specification for the end-users hardware (e.g. PCs and scanners) – technical documentation which shall include aspects related to: • The System Architecture Document describing the models in UML language to include at least the following (with sufficient level of detail): • Analysis Model, including: - Requirements model and/or use case model; - Domain Model, fully specifying the entities and the relations between them; - Component Model, including narrative description of all components, the links between them and integration interfaces with other systems/external components. • Logical Model, including: - Class Diagrams - Data Model • Deployment Model, including narrative description of all nodes and the links between them. This model will also contain the precise specifications of equipment and operation environments for the operation of the system at normal parameters, as well as specifications for a minimal configuration; • Dynamic Model to include: - Diagrams and narrative description of the states and transitions of the key entities; - Activity Diagrams and/or sequence for the key use cases.	Week 6
3	Detailed technical requirements for the needed hardware (servers, storages, networking, etc) as well as for the end-users (e.g. PCs, barcode scanners, printers, if any)	Week 4

Identifier	Description / Explanation	Estimated Deadline
4	Testing documentation. Functional, performance and security testing reports. Full package of unit tests;	Week 29
5	System installation and configuration guidelines (to include at least how to install application, what the hardware and software requirements are, platform description and configuration, application configuration, disaster recovery procedures);	Week 34
6	Compiled and documented source-code (including third instruments and libraries, where applicable)	Week 34
7	Software installation package (including third instruments and libraries, where applicable)	Week 34
8	Software licenses (where applicable);	Week 34
9	Documentation of APIs used for integration with other IT systems;	Week 34
10	Manuals for users and administrators as well as training materials (in Romanian);	Week 39
11	Operation Manual in Romanian	Week 39
12	Support period for at least 12 months; Patching of security flaws (at application level); Fixing of defects; Investigation of errors detected during system operation; Regular delivery of maintenance and support reports.	(12 months after operational acceptance)
13	Monthly Progress Reports	Monthly

Users' Manual

The Contractor's team shall include a printable manual book that provides instructions and guides to MJ, Forensic

institutions as well as other users on how to use the new software system.

The Users' Manual shall be distributed electronically in PDF format.

The Users' Manual should be written for the average user who may have a middle level of computer skills and shall contain at least a detailed explanation of the use of the System, detailed responsibilities of each user role, System's functionalities and other appropriate information.

The Users' Manual must be available in Romanian language.

The Users' Manual should be dual purpose to serve as a desk companion or library resource and as a training material for any training course that may be conducted. In the case of a training course, the Users' Manual would be printed and distributed to the training participants.

System's on-line Help

The new System should provide an on-screen refresher guide that covers critical topics from the user guide to help the user whilst he or she is currently logged in. The logged in user should be able to access the online help section in any event that the user does not have immediate access to the operation manual.

The online help section should not be a duplication of the entire contents of the operation and maintenance manual. Specific topics deemed critical should be the priority in the online help section. Thus, online help provides a limited set of topics to read through.

Administration Manual

The software development team shall prepare and deliver the System installation and configuration guidelines (to include at least how to install application(s), what the System's hardware and software requirements are, platforms description and configuration, application configuration, disaster recovery procedures).

The Administration Manual shall describe entire set of components and controls used for the configuration of the new System, including also the guidelines to the System Administrators on how to manage the users and their roles.

Also, the Administration Manual shall provide instructions on System's maintenance and all back-up aspects.

Operation Manual

The Operation Manual is document designed for the developers, which has to provide good understanding and guidelines on how the software system is organized and how further adjustments can be made. In other words, the aforementioned manual is intended for programmers wishing to customize or extend the delivered System or interact with the System's APIs. Programmers wishing to extend or customize the System are expected to know and understand the technology and the programming languages as well as object-oriented design principles. It is also expected that the wishing to extend or customize the System are familiar with HHTPS, HTML, CSS and XML.

The database developers that intend to extend or customize the databases of the System must have good knowledge of DBMS as well as good skills in respective transaction language (e.g. T-SQL).

This operational manual shall describe the programming style and practices used in the development of the System. Any developers that intend to extend or customize the System in the future must conform to the guidelines of the

manual and their source code shall be made available to the System Administrators.

The operational manual has to approach at least the following aspects:

- Requirements to the environment;
- System's Requirements;
- Development Tools to be used;
- Namespaces;
- Vocabulary;
- System's settings and Configuration Rules;
- System's components;
- Third-party components;
- System's APIs if any;
- Other aspects relevant for system's developers.

Testing documentation

The Contractor's testers' team are responsible for the documentation of artefacts created before or during the testing of the System. It must help the testing team to estimate their testing effort, test coverage, resource tracking, execution progress, and other aspects related to the software testing.

The documentation must contain a complete suite of documents that would allow describing and documenting test planning, test design, conducting of tests, as well as documenting test results that are drawn from the testing activity.

The Contractor shall prepare the testing documentation in close cooperation with the software developers and the Beneficiary's approval. In this sense, the testers' team shall prepare and deliver the following documents:

- Test Plan as a complete planning document, which contains the scope, approach, resources, schedule, etc. of testing activities. In other words, the Test Plan shall outline the test strategy and overall testing approach for the new System. It must describe the objectives of the testing, resources allocated for testing, time estimation and the templates of the deliverables as outputs of the testing activities. It must give guidelines how the testing will be conducted, to ensure the needed quality of the new System.

- Test scenario(s) – item or event of the new System, which could be verified by one or more Test cases;

- Test Case(s) – a group of input values, execution preconditions, expected execution post-conditions and results. This must be prepared for each test scenario. The general structure of each test case shall consist of at least the following:

    - Unique ID and title of the test case;
    - The description of the test case (e.g. narrative description of the user's functionality, operation);
    - Preconditions;
    - Dependencies;
    - Actor (user role);
    - Expected result;
    - Steps to be undertaken by the user in order to achieve the expected result;
    - Exceptions, if any.

- Testing Report(s) – a summary report document which summarizes testing activities conducted as well as the test results and well documented identified deficiencies (e.g. bugs, exceptions, etc.) in the new System, which fails to perform its expected function and produce the expected results;

- Action Plan for fixing the identified deficiencies – the list of the proposed actions such as software debugging/development activities in order to fix the identified deficiencies in the Testing Report. The proposed actions shall be prioritized according to the severity of the identified deficiencies (e.g. critical or high-severity, medium, low);

- Report on implemented Action Plan for fixing of the identified deficiencies – a short summary report, which

must reflect the list of the fixed deficiencies versus identified deficiencies as per action plan mentioned above.

Other Technical Documentation

At least the following documents shall be prepared and submitted by the software development team after the System is developed and tested:

Deployment Model, including the description of all nodes and the links between them. This model shall also contain the precise specifications of equipment and operation environments for the operation of the system at normal parameters, as well as specifications for a minimal configuration;

- Final System Architecture (as-built);
- Well commented Database structure, data models, including the SQL creation script;
- Documentation of the developed APIs (if any) used for the data exchange with other ICT systems/databases;
- Any other technical specifications that are relevant to the newly developed System.

14. SYSTEM TESTING AND QA

The Bidder /Contractor shall prepare and submit in his proposal the methodology and procedures specifying details how he intends to design and install Beneficiary specific Information Management System.

Methodology that shall include details about needed for information technologies (hardware, system software, general purpose software, application software, standard software, custom software, etc.) and services testing activities. The methodology shall be updated after signing of the Contract Agreement and adapted to the Project Plan after receipt of acceptance from the Beneficiary.

Special attention shall be drawn by the Contractor during the Methodology preparation and during implementation to Beneficiary requirements related to the integration of the already developed procedures and processes to the new System and uninterruptable operation of the current system until commissioning is completed by the Contractor.

The Bidder / Contractor shall demonstrate that the proposed methodology and procedures they will use fully cover the topic of the project so that it is possible to test all the functionalities identified and agreed with the Beneficiary in the Auditing, system analyses and design phase.

14.1. Inspections

Contractor shall keep a system development version in the Development Environment.

At least 70% of the developed specific system components shall be subjected to unit testing.

Contractor shall regularly update the components of the development environment and support the regular reports with system demos.

Contractor shall document and address the UNDP's and MJ's requests that will be classified into defects and modification requests if appropriate.

Inspections at system delivery stage

To perform the delivery Contractor shall install the system components on an Integrated Environment (according to the configuration requested by the MJ).

Contractor shall install the system components according to the installation guidelines.

Contractor shall install the system components together with the Beneficiary's system administrator.

Contractor shall configure the system components on the integrated environment.

Contractor shall modify the configuration parameters according to the installation guidelines.

Contractor shall modify the configuration parameters together with the system administrator.

Contractor shall demonstrate the functionality of all the system components.

14.2. Performance Testing

In addition to the Contractor's standard check-out and set-up tests, the Contractor (with the active engagement of the Beneficiary) shall perform the tests on the System and its components/subsystems before installation will be deemed to have occurred and the Beneficiary will issue the Installation Certificate(s).

Beneficiary will check if all the automatic mechanisms of integration with other computer subsystems meet the requirements.

The Contractor will perform the accessibility testing according to the Web Content Accessibility Guidelines (WCAG) 2.0.

The Contractor shall provide details about the testing method and the achieved results.

The Contractor shall perform the security testing at least according to OWASP Top 10 vulnerabilities[6].

The Contractor shall provide details about the testing method and the achieved results. Contractor will conduct the performance testing at least for two components:

- load testing;
- stress testing.

Beneficiary may request an expertise of the testing results from third parties.

The acceptance criteria for pre-acceptance testing are:

- 100% of the nonconformities detected at delivery were addressed;
- 80% of the accessibility tests for A level are successful;
- 100% of the security tests are successful;
- performance is better than required;

The acceptance date will be the point when all the nonconformities detected when the system is put into production have been addressed.

14.3. Operational Acceptance Testing

The Contractor shall prepare and submit all needed documentation for tests and Operational Acceptance Tests procedures in advance – at least one month 2 weeks before testing. The exact deadline shall be agreed in the detailed implementation plan.

The Beneficiary (forensic institutions and MJ), assisted by the Contractor will perform the following tests on the System and its components following installation to determine whether the System meets all the requirements mandated for Operational Acceptance.

The Beneficiary and Contractor will check the entire business-cycle and the related technical performance through operational tests.

The operational acceptance criteria's when the Beneficiary shall consider accepting the System are as follows:

- all the positive scenarios have been successfully performed and operation;
- at least 80% of the negative scenarios must be successfully handled;
- there are no high-severity or critical bugs[7];
- no testing scenario will corrupt the data integrity.

The system shall be deemed as accepted when it will operate according to the normal parameters and no major operation deficiencies[8] are operation and detected at least during three months.

Major deficiencies shall be considered the errors that cause obstruction of system functionalities that prevents avoiding or overcoming a situation that requires the involvement of the System Administrator or even system developers.

[6] The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.
[7] High-severity or critical bugs are those errors that render the System or its functionality unusable and have no workaround, cause loss and/or corruption of stored data, cause database deadlocks or blocking situations so that the user become unable to continue his work in the System.
[8] Major deficiencies shall be considered the errors that are not in line with the System functionalities and require avoiding or overcoming a situation with the involvement of the System Administrator or even software developers.

15. PRELIMINARY IMPLEMENTATION SCHEDULE

The following is the indicative list of tasks and schedule:

	Subsystem / Item	Involved Parties	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Milestone
	INCEPTION				
	Prepare and submit the Preliminary Project Plan of the FCMS. Approval of the Project Plan.	Contractor, UNDP, MJ, forensic institutions	W0	W0	Yes
	PHASE I				
	Hold workshops and meeting with the stakeholders' subject-matter experts and prepare a detailed requirements specification (SRS, SDS, etc)	Contractor, MJ. Forensic institutions	W1	W6	Yes
	Prepare detailed technical requirements for the needed servers and other hardware infrastructure	Contractor	W1	W4	No
	Preparation of technical specification for the end-users' hardware (e.g. PCs and scanners).	Contractor	W1	W4	No
	Prepare the detailed implementation plan for the FCMS	Contractor	W4	W5	Yes

	Subsystem / Item	Involved Parties	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Milestone
	Defining data sets operated in FCMS that shall be exchanged with other ICT systems/DBs.	Contractor	W4	W6	No
	PHASE II				
	Establishment of the configuration/development and testing environments.	Contractor, ITCSS	W7	W8	No
	Development/Configuration of the FCMS IS functionalities according to the prepared detailed requirements specification (SRS + SDS).	Contractor	W9	W22	Yes
	Integration with the shared e-services and interoperability platform MConnect.	Contractor, eGA, ITCSS, MJ	W20	W22	No
	Implementation of the interfaces for data exchange with other external ICT systems.	Contractor	W22	W23	No
	Final configurations of the System.	Contractor	W23	W24	No

	Subsystem / Item	Involved Parties	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Milestone
	Testing of the FCMS IS software solution: Performance and Security testing; Functional Testing.	Contractor, MJ, forensic institutions	W25	W29	Yes
	Training of the selected users from MJ and Forensic institutions;	Contractor, MJ, forensic institutions	W29	W29	Yes
	PHASE III				
	Final configurations and tuning of the FCMS	Contractor, MJ, forensic institutions	W30	W34	Yes
	Training on using the FCMS IS functionalities according to the ToT approach (both for the end-users and System Administrators from ITCSS);	Contractor, MJ, forensic institutions	W35	W39	No
	Final Acceptance of the FCMS	Contractor, UNDP, MJ, forensic institutions, ITCSS	W40	W42	Yes
	PHASE IV				

	Subsystem / Item	Involved Parties	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Milestone
	Technical support to correct any shortcomings related to the functioning of the System for a period of 12 months after the acceptance of the first version.	Contractor	W43	(12 months after operational acceptance)	No
	Troubleshooting of problems related to the development/configuration of the FCMS IS functionalities not identified during testing and acceptance phases in a warranty period.	Contractor	W43	(12 months after operational acceptance)	No
	Additional knowledge transfer if it is deemed necessary by the MJ staff in the warranty period.	Contractor	W43	(12 months after operational acceptance)	No
	Post-implementation support according to the requirements and the SLA specified within the 2.5 Service Specifications	Contractor	W43	(12 months after operational acceptance)	No
	Provide any available updates and upgrades to the installed IT solution, including DBMS, and other software components.	Contractor	W43	(12 months after operational acceptance)	Yes

16. REQUIREMENTS REGARDING THE FORMAT OF THE TECHNICAL PROPOSALS

16.1. Description of the Proposed ICT Solution

The Bidder must provide detailed descriptions of the essential technical, performance, or other relevant characteristics of all key Information Technologies, Materials and Services offered in the tender (e.g., version, release, and model numbers). Without providing sufficient clear detail, Bidders run the risk of their tenders to accumulate the minimum technical score.

To assist in the tender evaluation, the detailed descriptions shall be organized and cross referenced in the same manner as the Bidder ’s item-by-item commentary on the Technical Requirements described in Section below. All information provided by cross reference must, at a minimum, include clear titles and page numbers.

16.2. Item-by-Item Commentaries on the Technical Requirements

The Bidder must provide an item-by-item commentary on this Technical Requirements, demonstrating the substantial responsiveness of the overall design of the System and the individual Information Technologies, Goods, and Services offered to the Requirements.

In demonstrating the responsiveness of its tender, the Bidder is strongly urged to use the Technical Responsiveness Checklist provided in Section below of the Technical Requirements.

Failure to do so, increases significantly the risk that the Bidder ’s Technical Tender will result in a lower technical score. Among other things, the checklist shall contain explicit cross references to the relevant pages in the Bidder ’s Technical Tender.

16.3. Technical Responsiveness Checklist

The following Checklist is provided to help the Bidder organize and consistently present its Technical Tender. For each of the following Technical Requirements, the Bidder must describe how its Technical Tender responds to each Requirement. In addition, the Bidder must provide cross references to the relevant supporting information, if any, included in the tender. The cross reference shall identify the relevant document(s), page number(s), and paragraph(s). The Technical Responsiveness Checklist does not supersede the rest of the Technical Requirements (or any other part of the Tender Documents). If a requirement is not mentioned in the Checklist, that does not relieve the Bidder from the responsibility of including supporting evidence of compliance with that other requirement in its Technical Tender. One- or two-word responses (e.g. “Yes,” “No,” “Will comply,” etc.) will be not considered by the Employer to be sufficient to confirm Contractors technical responsiveness with Technical Requirements.

Template for technical responsiveness checklist:

Tech. Require. FRQ000 or NFRQ000	Technical Requirement:	Mandatory
Bidder ’s technical reasons supporting compliance:		
Bidder ’s cross references to supporting information in Technical Tender:		

16.4. Preliminary Implementation Plan

The Bidder must prepare a Preliminary Implementation Project Plan describing, among other things, the methods and human and material resources that the Bidder proposes to employ in the design, management, coordination, and execution of all its responsibilities, if awarded the Contract, as well as the estimated duration and completion date for

each major activity. The Preliminary Implementation Plan must also address the topics and points of emphasis specified in this document. The Preliminary Implementation Plan shall also state the Bidder 's assessment of the major responsibilities of the Beneficiary and any other involved third parties in System supply and installation, as well as the Bidder's proposed means for coordinating activities by each of the involved parties to avoid delays or interference.

In addition to the topics and points of emphasis, the Preliminary Implementation Plan must address all activities listed in the Implementation Schedule.

Confirmation of Responsibility for Integration and Interoperability of Information Technologies.

INSTITUTIONAL ARRANGEMENTS

The Service Provider will work under the guidance of the UNDP Project Manager for substantive aspects of the assignment and under the direct supervision of the UNDP Project Officer for administrative aspects.

The Service Provider is expected to cooperate closely with the representative of the Ministry of Justice, management and delegated staffers from the National Centre for Judicial Expertise under the Ministry of Justice, Forensic and Judicial Expertise Centre under the General Police Inspectorate, Centre of Legal Medicine under the Ministry of Health, Labour and Social Protection; National Anticorruption Centre; Moldovan Border Police, private forensic experts' bureaus.

All the deliverables shall be submitted in English and Romanian language, in hard copy and electronic format.

Before submission of final deliverables, the Service Provider will discuss the draft documents with the parties involved, so that the final products reflect their comments. All the deliverables of the Service Provider shall be coordinated with the A2J project team.

COVID-19 implications

As of 11 March 2020, the World Health Organization (WHO) declared COVID-19 a global pandemic as the new coronavirus rapidly spread to all regions of the world. Travel to and in the country has been also subjected to restrictions of different duration and scope, since March 2020.

The selected Service Provider shall abide by the latest recommendations of WHO and National Commission for Emergency Situations of the Republic of Moldova pertaining to safety measures in the COVID-19 context.

Please note that the Project Team envisages as most the efficient approach for carrying out the assignment the on-site working, in particular when it comes to conducting of activities related to the Analysis and Design phase, as well as when conducting of users' trainings. When planning and conducting workshops/meetings with physical presence of participants, the Contractor shall abide by the safety rules and regulations set by the Moldovan authorities in regard to gatherings/meetings at that particular time, ensuring the safety of its staff and those they shall interact with. Hence, no stakeholders, consultants or UNDP staff should be put in harm's way and safety is the key priority.

It is also expected the Contractor to ensure a fast response during the technical support period especially for the most critical issues signaled by the FCMS users. Therefore, it is desirable for the Bidder to have local office or a local consortium partner or a local subcontracted consultant or local subcontracted company in Republic of Moldova which will serve as a local contact point in order to ensure the fastest reaction of the Contractor when so required.

However, in case of limited possibilities to travel or on-site working restrictions due to COVID-19 epidemiologic situation within the country, the Service Provider should develop a methodology to conduct the assignment virtually and remotely, using teleconferencing equipment and tools, including the use of remote interview methods and extended desk reviews, data analysis, surveys and evaluation questionnaires.

In this context while preparing and undertaking interviews, meetings, presentations and briefings through telephone

or online (skype, zoom etc.) the Contractor shall work remotely in close coordination with the Project team.

The above noted aspects shall be detailed in the inception report and agreed with the A2J project team. The limitations like stakeholder availability, ability or willingness to be interviewed remotely, accessibility to the internet/ computer and working from home arrangements must be reflected in the final report.

The Offeror's proposal shall be clear on the activities, costs entailed, and approach proposed to ensure the delivery of the assignment in the current pandemic context whereby objectives of the assignment are met, while enforced safety standards are adhered to.

Three missions (*deemed necessary for design or completion of assignment tasks and/or deliverables*) may be considered only when it is confirmed to be safe for staff, consultants, stakeholders and if such missions are possible within the assignment's schedule. The exact duration and period of the missions shall be coordinated with UNDP.

For purpose of estimation of services' costs, the expected duration of the mission, could be up to 10 working days, depending on the scope.

In line with the UNDP's financial regulations, when determined by the UNDP Moldova Country Office and/or the Service Provider that a deliverable or service cannot be satisfactorily completed due to the impact of COVID-19 and limitations to the assignment, that deliverable or service will not be paid.

However, due to the current COVID-19 situation in the country and its implications, a partial payment may be considered if the Service Provider invested time towards the deliverable but was unable to complete to circumstances beyond his/her control.

Language requirements:

All documentation related to the assignment shall be in English and Romanian. All documents submitted, in English and Romanian, will be subject to proofreading and editing to ensure compliance with the language and terminology in the national legislation regulating the subject matter of the assignment.

The Service Provider shall ensure, if necessary, interpretation during interviews, meetings, presentations and briefings organised through telephone or online, during the missions, to the Republic of Moldova, should these be organised, as well as translation of assignment related documentation and deliverables.

Any translation, interpretation and proof-reading costs shall be listed separately in the financial proposal.

17. QUALIFICATIONS REQUIREMENTS

The bidder shall provide sound argumentation of the proposal by demonstrating compliance with the ToR and the environment in which it will provide the services. The bidder shall include information on the volume of allocated resources to carry out the assignment.

A breakdown per working days allocated for each deliverable shall be submitted, clearly explaining the role of the team members involved in producing the deliverable. In this context, the Service Provider shall ensure a clear presentation of distribution of tasks and allocation of working days deemed necessary for engagement.

The proposed team should consist of but not be limited to the following members:

- Project Manager:
- Technical Team Leader
- Software Architect:
- Lead Business Analyst
- Database Developer
- Software Tester Engineer

Successful bidder shall meet the following minimum qualification requirements for the assignment:

Minimum Eligibility and Qualification Criteria

Criteria for the evaluation of the Bidder:

- Legally registered entity or consortium of companies that can ensure rapid local response (including presence of staff) to any of the contract related requests (whether though a local branch or office, through a local consortium partner or a local subcontracted consultant or company or other);
- Minimum 5 (five) years of experience in ICT solutions development.
  (For JV/Consortium/Association, the below should be met:
  - The Lead Partner of the JV shall demonstrate that he has a minimum of 5 years of experience in ICT solutions development;
    The other consortium partners shall demonstrate that they have a minimum of 3 years of experience in ICT solutions development).
- Minimum 2 (two) successfully executed ICT projects of similar complexity, where at least one project implemented for state bodies (i.e. central public authorities, state agencies, etc.) (i.e. highly configurable case management systems, document and workflow management systems) implemented over the last 5 (five) years. The Bidder shall present proofs of projects completion with his Proposal.
- Demonstrated experience of working with Moldovan public institutions would be a strong advantage
- Working experience with UN Agencies and/or other international organizations will be an asset

Criteria for the evaluation of key project personnel:

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

1	**Project Manager:**
	Master degree (or 5 (five) years university degree) in the field of Computer Science and/or Information Technologies or related areas

	At least 5 (five) years of professional experience in the field of design, development and implementation of complex software solutions
	At least 2 (two) similar successfully completed ICT projects with similar complexity, in a leading role throughout the entire duration, proven by brief descriptions of project scope and outcome, and proofs of completion
	Internationally recognized project management certification such as PMP, PRINCE2, AGILE or equivalent
	Fluency in English. Knowledge of Romanian or Russian is an asset
2	**Software Architect**:
	Master's degree (or 5 (five) years university degree) in the field of Computer Science and/or Information Technologies
	At least 5 (five) years of professional experience in designing and implementation of IT systems architecture, including large-scale architectures
	Engagement in at least 2 (two) projects for implementation of various ICT solutions that involved document management and business-process management, as System Architect, proven by brief descriptions of project scope and outcome, and proofs of completion
	Fluency in English. Knowledge of Romanian or Russian is an asset
3	**Lead Business Analyst**
	Master's degree (or 5 (five) years university degree) in the field of Computer Science and/or Information Technologies or related areas
	At least 5 (five) years as a Business Analyst for ICT solutions
	Engagement as Business Analyst in at least in at least 2 (two) projects for the implementation of complex software web-based BPM and/or DMS solutions, proven by brief descriptions of project scope and outcome, and proofs of completion
	Strong experience and knowledge on business-processes modeling in the content of IT systems and experience in user requirements elicitation
	Internationally recognized certification in Business Analysis issued by an internationally recognized institution proving advanced knowledge regarding requirements' identification, analysis, prioritizing, management, communication, verification and validation (i.e. BPMT, CBAP or equivalent) is a strong asset.
	Fluency in Romanian is a must. Knowledge of English or Russian will be an asset
4	**Database Developer**
	Master degree (or 5 (five) years university degree) in the field of Computer Science and/or Information Technologies
	At least 5 (five) years of overall professional experience in database design, development and administration
	Advanced knowledge on databases development and administration and DB security
	Advanced knowledge on databases' performance optimization on the database technology
	Professional certification in the Database technology on which the Tenderer's proposed FCMS solution is based
	Specific professional experience proved through participating in at least one similar project, within which he/she held a position of Database Developer
	Fluency in English. Knowledge of Romanian or Russian is an asset
5	**Technical Team Leader**
	Master degree (or 5 (five) years university degree) in the field of Computer Science and/or Information Technologies

	At least 5 (five) years of experience in the design, software development and implementation of complex software platforms
	Certification in software development technology and/or programming language(s) on which the bidder's proposed solution is based (*no certification – 0 pts; certified expert – 15 pts)*
	Fluency in English. Knowledge of Romanian or Russian will be an asset
6	**Software Tester Engineer**
	Master degree (or 5 (five) years university degree) in the field of Computer Science and/or Information Technologies
	At least 3 (three) years as a Quality Assurance Expert
	Experience in at least 2 (two) projects, in which provided Quality Assurance services for software solution, proven by brief descriptions of project scope and outcome
	Recognized certification at international level regarding advanced competences related to setting the optimal testing activities based on risk analysis of information systems and tests execution depending on the particular methodology for software development
	Fluency in English. Knowledge of Romanian or Russian is an asset

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

UNDP Moldova is committed to workforce diversity. Women, persons with disabilities, Roma and other ethnic or religious minorities, persons living with HIV, as well as refugees and other noncitizens legally entitled to work in the Republic of Moldova, are particularly encouraged to apply. Applicants demonstrating equitable gender representation and diversity within the team will have an advantage.

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

Bidders agree that experts will provide high quality outputs and expertise and participate in the project at the level and duration specified. Thus, a Statement of Availability shall be provided for this purpose. Should any changes be necessary in this regard, a formal request for the agreement of the A2J Project team to allow substitutions, shall be submitted.

UNDP may at any time request the withdrawal or replacement of any of the Service Provider personnel. Replacement will be at the Service Provider expense.

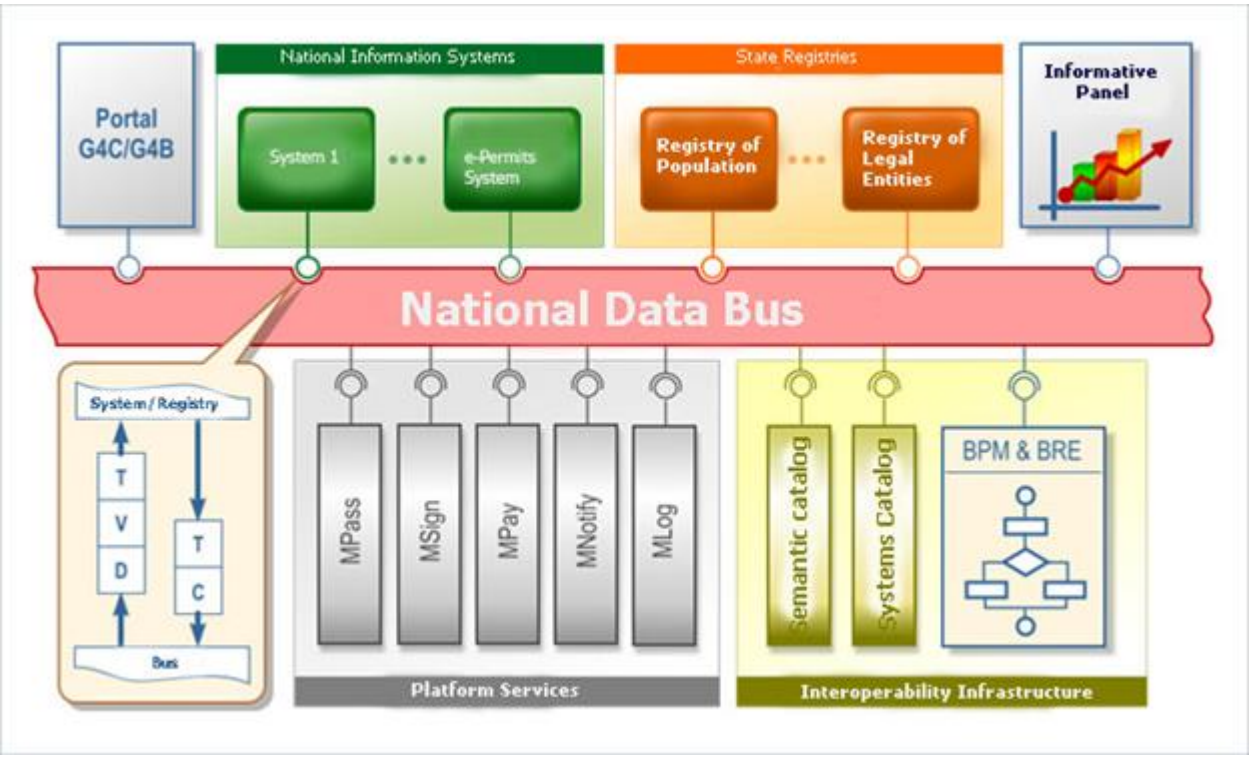
18. ANNEXES

18.1. Governmental ICT Infrastructure

MCloud – Governmental Cloud Infrastructure

Many digital solutions designated for the Moldovan's public sector use the existing e-Government infrastructure and shared electronic services, as follows:

- Governmental Cloud (MCloud)
- Enterprise Content Management Platform (ECMP);
- Government Authentication Platform (MPass);
- Digital Signature (MSign)
- Service for Electronic Payments (MPay);
- Logging Service (MLog);
- Notification Service (MNotify);
- Interoperability Government Platform (MConnect);



Existing Governmental ICT Infrastructure

Cloud government infrastructure - "MCloud" is a fully virtualized environment based on VMWare.

Hosting ICT solutions in MCloud is the only plausible and legal proposal, as the scenario saves beneficiaries from significant infrastructure costs, such as: data centre creation, purchases of servers, storages, networking devices, security and so on. The entire MCloud infrastructure is a government-owned one, created especially for the country's public authorities and institutions. Being managed by the ITCSS, it is one of the most secure and equipped ICT infrastructures in the country.

Placing of any ICT solution in MCloud saves the system's owner from additional hardware maintenance costs. This being transferred under the responsibility of the technical administrator.

It is worth mentioning that MCloud was specially designed and built so that several institutions can use

common ICT solutions and applications, stored in a single data centre. None of the institutions needs server infrastructure and storage space.

The Government of the Republic of Moldova has launched the common technological platform MCloud, especially to streamline spending on the consumption of ICT services. The MCloud platform comes to capitalize on government costs and consolidate data centers into a form of shared management. Thus, considerably reducing costs and increasing the quality and security of information systems of state importance.

The MCloud platform has been fully operational since February 14, 2013, and many public authorities have already migrated digital content to this platform.

MPass

MPass is the national service, which allows authentication and access to digital public services. The service offers different authentication mechanisms: mobile signature, digital certificate, user name and password.

MPass Server offers a Single Sign-On authentication that provides users with full control over the authentication and authorization of hosted user accounts.

It is important to note that the potential solution which uses single-sign-on, only applies to web applications and applications, which requires direct or indirect user interaction with MPass website.

Users which have valid digital certificates are be able to create accounts that do not need validation. The MPass server automatically extracts data from the trusted digital certificate and creates a validated user account.

Any digital solution which integrates MPass service will be required to assign a certain level of authentication. Thus, systems which require high assurance of user identification will be requesting authentication with client digital certificate and those which consider the login/password as sufficient will allow both forms authentication and digital certificate authentication

Electronic Governance Agency shall provide the MPass Integration Guide, which provides a high-level view on the system architecture, and details the process of system interaction to provide authentication services to third party IT Systems and Service Providers.

MSign

MSign is the government's electronic signature service, which offers the ability to use all types of electronic signatures in online interactions and verify the authenticity of signatures under guaranteed security.

Through MSign the user can sign with 3 available tools: Mobile Signature, Electronic Identity Card and Electronic Signature (ITCSS).

The ICT solution shall be integrated with MSign to be used in particular for the signing of documents within the digital applications and in order to certify some users' actions.

One of the electronic signature tools is the Mobile Signature, which was launched in September 2012, in partnership with mobile operators in the Republic of Moldova. It provides digital signature and timestamp over time. MSign is integrated with many information systems in Moldova for accessing electronic services and allows users to sign various digital content like web forms, offline documents, images.

Mobile signature is an innovative service that allows access to electronic services using a mobile phone. It works as an identity card in the virtual environment, allows authentication in the virtual space to confirm the

identity with the help of the mobile phone.

With the help of the mobile signature, users can sign remotely documents, reports, statements or online applications. Both public and private electronic services can be also accessed in a simple and convenient way. Users do not depend on the work schedule of the institutions, but can access electronic services from anywhere and anytime.

According to law no. 264 of July 15, 2004 regarding the electronic document and the digital signature, the documents in electronic format are equivalent to the handwritten paper documents.

To obtain the right to digital signature via mobile phone, certificates issued by the Information Technology and Cyber Security Service are used, and the right to register users is granted to mobile operators.

Anyone can quickly get the mobile signature from the mobile operators in the Republic of Moldova. For this, they shall present only the identity card and complete an application. This process does not take more than 15 minutes. The regular SIM card that MD citizens have is usually replaced with a special SIM card, which includes the mobile signature.

MLog

MLog is a centralized service which aims to provide a secure and flexible mechanism for logging and auditing, ensuring conservation of the transactions (events), produced in an information system at a given time.

Electronic Government AGency will provide the MLog Integration Guide, which describes the technical interfaces that must be exposed by information systems that integrate with MLog and the technical interfaces that MLog exposes for them

MNotify

MNotify is a software application for sending of notifications within the information systems owned by public authorities within their jurisdiction and other public institutions of public service.

In this context, "Service" implies a message that is automatically generated by the information systems of the institutions with the purpose to notify users about changes of certain services or methods of service provision.

Thus, users may be notified of any changes in terms of reduced time, by e-Mail, SMS, instant messaging or other communication channels, as needed.

Electronic Government Agency will provide the MNotify Integration Guide, which describes the technical interfaces that must be exposed by information systems that integrate with MNotify and the technical interfaces that MNotify exposes for them.

Governmental Interoperability Platform – “MConnect”

The Governmental Interoperability Platform “MConnect” facilitates the exchange of data between the authorities to increase the efficiency and quality of delivery of public services. Through the interoperability platform, the public authorities exchange data in real time without requesting it from citizens and the business environment in the form of certificates, reports and other types of documents.

‘MConnect’ ensures the following objectives:

- increase the efficiency and effectiveness of information systems through which electronic public

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

The data exchange will be performed through secured channels, using dedicated standards and protocols such as XML, SOAP and HTTPS. MConnect is compatible with the following databases:

- Microsoft SQL Server;
- Oracle;
- MySQL;
- Informix;
- DB2;
- …and other relational databases; as well as with:
- Cassandra,
- MongoDB and other non-relational databases.