_____
(RESTRICTED – if applicable)

APPROVED BY
System Owner

Deputy Head of the SJA of Ukraine
for Digital Development, Digital
Transformation and Digitalisation

_____Leonid SAPELNIKOV
(position, signature, first name, SURNAME)
‘____’ _____202__

TECHNICAL REQUIREMENTS

FOR THE CREATION OF THE INFORMATISATION TOOL — THE ‘ACCESS MANAGEMENT’ COMPONENTS, CORE SERVICES AND INFRASTRUCTURE OF THE UNIFIED JUDICIAL INFORMATION AND COMMUNICATION SYSTEM

(select the purpose and indicate the full name of the information and communication system)

Project Code: UJICS — Core Services and Infrastructure
(ICS code)

On ___ pages

AGREED BY

Developer of Technical Requirements

Executive Director of the NGO ‘Agency for Legislative Initiatives’

_____ Svitlana MATVIIENKO

(position, signature, first name, SURNAME)

‘____’ _____202__

CONTENTS

1 GENERAL PROVISIONS

1.1 Basis for Developing the Technical Requirements

Ukraine has been undergoing an active process of judicial reform in recent years. This has created a need to improve and expand the tools used to automate the activities of judicial institutions. The decision to establish and further modernise the Unified Judicial Information and Communication System (hereinafter, the 'UJICS') was driven by the need to provide sustained support for the digital transformation of Ukraine's judicial system in line with the State's strategic justice-sector objectives, including improving the accessibility of judicial procedures, accelerating court proceedings and enabling comprehensive online interaction between participants in proceedings and the courts.

The current state of the electronic court system does not meet these objectives. At present, the system operates as a set of independent subsystems and standalone solutions developed at different times, with absent or limited integration and varying levels of information security. This fragmentation prevents the establishment of a single information environment for the judiciary, causes integration issues and duplication of functionality and complicates the further development of the system.

Some solutions are based on technologies that do not meet current requirements for scalability, performance, reliability and information security. Continued use of such components creates risks of system failures and data loss, while also limiting the ability to introduce new functionality.

The practice of partial upgrades and local enhancements to individual solutions does not resolve systemic issues. On the contrary, it leads to the accumulation of technical debt. In the absence of a single architectural foundation, such solutions only temporarily mitigate individual problems while increasing maintenance complexity and support costs.

Accordingly, further development through fragmented enhancements is not appropriate. The strategic objectives of the digitalisation of the judicial system can be achieved only through the creation of a new, integrated and architecturally coherent information and communication system in accordance with the UJICS Concept.

1.2 Name of the Informatization Tool

Full name of the System: Unified Judicial Information and Communication System

Abbreviated name: UJICS

The terms 'System' and 'UJICS' shall be used interchangeably.

1.3 Purpose of Creating the Informatization Tool

In order to ensure the coherent, secure and efficient operation of the UJICS and to prevent fragmentation in approaches to access management, data management and infrastructure management, the UJICS requires the development and implementation of the following centralised shared components:

1. Core services:
    - 1.1. Access Management — IAM (Identity Access Management): management of users, organisations in the context of the user aggregator, roles, identification, authentication and authorisation, as well as recording access events for subsequent logging by the logging service;
    - 1.2. Reference Data and Classifiers — Dictionary: management of reference data, including classifiers and reference directories;
    - 1.3. Notifications — Notifications: informing users of events relevant to them within the System and/or within business processes automated by the System;
    - 1.4. Document Signing — Crypto Service: verification and application of qualified electronic signatures to objects, as well as consolidation of signed objects;
    - 1.5. Help and Guidance, Knowledge Base — Wiki: management of information materials, including articles, instructions and frequently asked questions;

1.6. Master Registers: organisations, organisational structure, positions, personnel and other relevant records.

2. A UNIFIED INFRASTRUCTURE shared by all UJICS components, which shall provide standardised approaches to deployment, operation, scaling, monitoring and information security.

Implementation of these components is a prerequisite for establishing an integrated, scalable and manageable UJICS architecture, reducing the costs of developing and maintaining UJICS components and ensuring consistent security standards and user experience.

1.4 Terms Used

The terms and abbreviations used in this document shall have the following meanings:

Term	Definition
Authentication	An electronic procedure that enables confirmation of the electronic identification of a natural person, legal entity, information system or information and communication system, and/or confirmation of the origin and integrity of electronic data
Authorisation	The part of the procedure for determining and granting access rights to functions and/or information resources within an information system following authentication
Administrator of the System	A legal entity whose remit, pursuant to its statutory powers or under a contract with the System Owner, is to implement organisational, technical and other measures necessary to ensure the support, administration and operation of the Informatization Tool.
API	Automated software integrations, also known as an ‘application programming interface’
Database or DB	An organised collection of data stored and managed using a computer system, which provides for the storage, organisation and access to data for the purpose of its efficient use and processing
Business process	A set of actions required to be performed by a person or a system in order to achieve a specified outcome
Validation	The establishment of objective and documented evidence that the specified requirements for a particular intended use can be consistently fulfilled
Website	A set of software tools hosted at a unique address in a computer network, including the Internet, together with information resources managed by specific entities and providing legal entities and natural persons with access to those information resources and other information services through a computer network
Verification	A set of measures for comparing, establishing compliance of and confirming information contained in information systems against information contained in the same or other systems, other State information resources, and information obtained, including through electronic interaction, from State authorities, local self-government bodies, enterprises, institutions and organisations that own and/or administer such information
VCS	Video conferencing subsystem
EDM	Electronic document management
UJICS	Unified Judicial Information and Communication System
ICS	Information and communication system
QES	Qualified electronic signature
CMU	Cabinet of Ministers of Ukraine
User	A person who has active access to the System’s functionality in accordance with their configured role

System	The informatization tool to which these Technical Requirements apply
UJICS components (components)	Information and communication systems, functional subsystems and components, their modules, shared core and infrastructure services, which form part of the UJICS and are intended to perform a specific functional task
TR	Technical Requirements. A document defining the planned needs of the System Owner and the general conditions for the creation, modernisation, modification, development, administration and operation of an informatization tool and containing a set of criteria describing that informatization tool
TS	Technical Specification. A document developed in accordance with the Technical Requirements that defines the purpose, quality indicators, technical and economic, technical and special characteristics of an informatization tool, and includes a description of operating processes, including business processes and the conditions for using the informatization tool
Trembita	The Trembita System of Electronic Interaction of State Electronic Information Resources
IAM	Identity and Access Management — an identification and access management module
BI	Business Intelligence subsystem within the UJICS
UJICS natural person (UJICS NP, NP)	A citizen of Ukraine, a stateless person or a national of another State whose personal data are registered in the UJICS for the purpose of that person's participation in processes automated by the UJICS. Not all UJICS NPs may be UJICS users. They may be registered in the UJICS solely for the purpose of being identified in documents or processes, while not being registered as users and not having rights to perform actions within the UJICS. For the purpose of maintaining records of such persons, the System shall contain an internal master register, the 'UJICS Register of Natural Persons', which manages NP record cards containing the personal data of NPs
Authorised UJICS user (user)	An identified and authenticated UJICS natural person who has been assigned a set of rights to perform actions within the UJICS. User records shall be maintained in the IAM service. A user account, also referred to as a user record card, shall contain the minimum necessary set of personal data required for identification and authentication, together with additional technical information concerning technical aspects of identification, authentication, authorisation, the legal statuses of the natural person, sessions and other relevant data. One user account shall correspond to only one active NP record card
User profile in the User Cabinet	A separate section or page in the User Cabinet through which a user may view their personal data and correct data that may be amended, view their current legal status and/or change it, review the functions available to them in accordance with assigned roles, view consolidated reference information from other UJICS components relevant to that user and initiate certain core processes
Legal status of a UJICS user (legal status)	A specialised information block indicating on whose behalf the user logs in to the System and intends to perform actions. Different legal statuses shall entail different sets of roles that may be assigned to the user during authorisation. Where the System cannot determine the user's legal status unambiguously using the available identification methods, the System shall explicitly request that information from the user during authentication. One and the same NP, as a user, may simultaneously have several legal statuses, for example, participate in divorce proceedings as a natural person and hold the position of a judge's assistant. However, within the System, such a user may work under only one specifically selected legal status at a time. The following categories of legal status shall be distinguished: • **Natural person**: the user intends to perform actions in the System as a private individual acting on their own behalf. Such a user may access information and perform actions relating exclusively to that individual as a natural person. Such users shall be identified using the Taxpayer Registration Number contained in the QES. • **Official:** the user intends to perform actions in the System as an official holding a specific position in an organisation within Ukraine's judicial system. A user with this legal status shall be assigned roles and rights corresponding to their official duties within that organisation and in that position. Accordingly, such a user may access information and perform actions relating exclusively to their official duties.

	Such users shall be identified using the Taxpayer Registration Number contained in the QES and, additionally, the Unified State Register of Enterprises and Organisations of Ukraine code of the organisation contained in the QES. Although concurrent employment in positions within the judiciary and State authorities is prohibited, technically, one employee may hold two positions: their main position and a temporary acting position while another employee is on leave or on a business trip. Where these positions entail different, and in particular conflicting, sets of roles, the System shall enable the user to select, during authorisation, the position under which they intend to work in the System. • **Representative:** the user intends to perform actions in the System and view information on behalf of and under the authority of a specific business entity, including a legal entity or sole proprietor, or another natural person. The System shall provide bilateral mechanisms for appointing representatives while ensuring compliance with all legal requirements applicable to that procedure. A user acting under this legal status may access information and perform actions relating only to the legal entity, sole proprietor or natural person whom they represent. Such users shall be identified using the Taxpayer Registration Number contained in the QES and additional attributes recorded during the appointment of a representative. In order to reduce technical errors, a user may represent only one specific business entity or one specific natural person during the same active System session.
Access context	A technical information block created as a result of the authorisation process in the IAM service and transmitted to UJICS components. It shall contain identification information about the user, the user's legal context and its details, the set of roles assigned to the user and technical parameters concerning the organisation of the user's System session. The complete list of access-context attributes shall be defined in the Technical Specification
Electronic Cabinet (EC)	A personal page of a User in the UJICS with the status of an official procedural instrument. It shall be used to identify a person and exercise their rights and obligations established by procedural legislation, including filing claims, receiving summonses and participating in video conferences. **Scope of application:** external communications between a court and a party to proceedings, as well as official actions by officials that have procedural consequences. **Legal basis:** the Law of Ukraine 'On the Judiciary and Status of Judges', the Commercial Procedure Code of Ukraine, the Civil Procedure Code of Ukraine, the Code of Administrative Procedure of Ukraine and the Criminal Procedural Code of Ukraine
User Cabinet (UC)	A generalised functional interface, or 'digital workplace', for any person registered in the System, including a court employee, an employee of the High Council of Justice, the High Qualification Commission of Judges of Ukraine, the State Judicial Administration of Ukraine or an external user. The User Cabinet shall provide a personalised view of the subsystems, modules and data available to the user in accordance with their roles and legal statuses. **Scope of application**: internal work, including administration, human resources and accounting, work with documents, analytics, as well as access to Electronic Cabinet functions. **Conceptual role**: for a citizen or an advocate, the User Cabinet shall be functionally equivalent to the Electronic Cabinet. For a court employee, the User Cabinet shall include both Electronic Cabinet functions and internal work tools, including the court document management subsystem and the personnel records subsystem.
Unified Personal User Environment (UPUE)	The technological shell and front-end architectural solution of the System that implements a 'single-window' concept for accessing all UJICS components. The UPUE shall provide a unified user experience, visual interface consistency and common navigation, serving as an environment for dynamically loading functional modules of different UJICS components without interfering with their internal business logic. It shall serve as the technological platform for implementing the functions of the Electronic Cabinet and/or User Cabinet, ensuring the integration of UJICS component interfaces into a single working environment.

1.5 Legal Framework

All requirements defined by this document shall comply with the regulatory and legal acts and standards listed in this section:

1. Constitution of Ukraine.
2. Law of Ukraine ‘On the Judiciary and Status of Judges’.
3. Law of Ukraine ‘On the High Council of Justice’.
4. Law of Ukraine ‘On the High Anti-Corruption Court’.
5. Law of Ukraine ‘On Prevention of Corruption’.
6. Law of Ukraine ‘On Civil Service’.
7. Law of Ukraine ‘On Information’.
8. Law of Ukraine ‘On Access to Public Information’.
9. Law of Ukraine ‘On Public Electronic Registers’.
10. Law of Ukraine ‘On Personal Data Protection’.
11. Law of Ukraine ‘On Electronic Documents and Electronic Document Management’.
12. Law of Ukraine ‘On Electronic Identification and Electronic Trust Services’.
13. Law of Ukraine ‘On Information Protection in Information and Communication Systems’.
14. Law of Ukraine ‘On the Basic Principles of Cybersecurity of Ukraine’.
15. Resolution of the Cabinet of Ministers of Ukraine No. 205 of 21 February 2025 ‘Certain Issues Concerning the Creation, Administration and Operation of an Informatization Tool’.
16. Resolution of the Cabinet of Ministers of Ukraine No. 764 of 28 June 2024 ‘Certain Issues Concerning Electronic Identification and Electronic Trust Services’.
17. Regulation on the Procedure for the Functioning of Certain Subsystems (Modules) of the Unified Judicial Information and Telecommunication System, approved by Decision of the High Council of Justice No. 1845/0/15-21 of 17 August 2021.
18. ISO/IEC 19510 — Information technology — Object Management Group Business Process Model and Notation, BPMN version 2.0.
19. ISO/IEC 1012 series — Requirements for testing electronic equipment.
20. ISO 9001 — Quality management systems — Requirements.
21. ISO/IEC 25010 — Systems and software engineering — Systems and software Quality Requirements and Evaluation, SQuaRE — System and software quality models.
22. ISO/IEC 8807 — Information technology — Telecommunications and information exchange between systems — Intra-domain routing protocol, IS-IS.
23. ISO/IEC 9126 — Software engineering — Product quality, predecessor to ISO/IEC 25010.
24. ISO/IEC 12207 — Systems and software engineering — Software life cycle processes.
25. IETF BCP 47 — standard for language tags in combination with country codes.
26. DSTU 4145-2002 — Information technologies. Cryptographic information protection. Electronic digital signature based on elliptic curves.
27. RFC 5545 — Internet Calendaring and Scheduling Core Object Specification, iCalendar.
28. NIST/FIPS series — standards of the United States National Institute of Standards and Technology and Federal Information Processing Standards, including standards on cryptography and cybersecurity.

2 PURPOSE OF THE INFORMATIZATION TOOL

2.1 Main Tasks and Functions of the Informatization Tool

The key functions of the System components shall include the following:

Ensuring the operation of the System as a single digital environment with centralised management of access, users, organisations and roles. The System shall provide for user identification, authentication and authorisation, maintenance of access and activity logs and management of reference and master data, master registers and classifiers as a single source of reliable data for all functional components of the System.

Ensuring the operation of the informatization tool within the UJICS unified infrastructure, which shall establish a shared technological environment for the deployment, operation and scaling of all System services. This infrastructure shall ensure the implementation of uniform approaches to monitoring, logging, configuration management and information security and shall support the reliability, continuity and manageability of System operations, taking account of scalability and fault-tolerance requirements.

The list of key functions is not exhaustive and may be further specified during the development of the Technical Specification.

2.2 Expected Results of Implementing the Informatization Tool

Implementation of the identification and access management modules, core reference data and shared services, as well as the unified infrastructure within the UJICS, shall enable the following results to be achieved:

- A single approach to access management: centralised authentication of users for all UJICS services, with segregation of roles and rights and service authorisation.
- Enhanced information security: reduced risks of unauthorised access, increased transparency of user actions and the ability to conduct a comprehensive audit of access events and System use.
- Harmonisation of reference data and functionality: the use of common reference directories and shared master registers shall ensure data consistency, reduce duplication of functionality and improve interoperability between services.
- Reduced development and maintenance costs: the reuse of shared components and unified infrastructure shall reduce the costs of creating, supporting and modernising UJICS components.
- Improved System scalability and manageability: consistent approaches to deployment, monitoring and operation shall enable the rapid connection of new UJICS components and the adaptation of the UJICS to changes in workload and functional requirements.
- Improved user experience: single authentication, consistent interaction interfaces and predictable behaviour of UJICS components shall simplify user activity and reduce operational workload.

2.3 Procedure for Developing the Informatization Tool

The UJICS shall be developed in stages, in accordance with the principles of modularity, scalability, interoperability and software component reuse. The current iteration of System development is intended to establish an architectural foundation, including the implementation of the Identity and Access Management module, core reference data and shared services, as well as the deployment of unified infrastructure. These components shall form the common technological environment and organisational basis for the operation of all UJICS components and shall establish consistent approaches to access management, information security and System operation.

Subsequent development iterations shall provide for the phased expansion of the functionality of existing modules and the implementation of new functional components in accordance with

identified priorities and user needs. The System shall be developed taking account of the need to integrate with existing information systems, ensure interoperability with external services and support new business processes and user scenarios.

This development approach shall ensure the incremental expansion of UJICS functionality without compromising the stability of core components, data integrity or continuity of System operation. It shall also enable the UJICS to adapt flexibly to changes in regulatory, organisational and technological requirements.

3 CHARACTERISTICS OF THE INFORMATIZATION OBJECT

The informatization object is the Unified Judicial Information and Communication System (UJICS) — an integrated information system comprising interconnected functional components, services and software and hardware facilities that automate the processes of courts, bodies and institutions within the justice system and enable electronic information interaction between them.

In order to ensure the consistency, coherence and cost-effectiveness of System operation and to prevent fragmentation in approaches to access management, data management and infrastructure management, the UJICS architecture shall provide for the implementation of a single centralised solution incorporating shared functional components and services that shall be mandatory for use by all UJICS components. This approach shall ensure the reuse of services and data, the uniform implementation of equivalent functionality and the continued currency of information.

The UJICS shared functional components shall include core services for managing user identification and access, maintaining reference and master data, notifying users of System events, verifying and applying qualified electronic signatures and managing knowledge and information materials. These components shall provide centralised management of access to System resources, recording and control of user actions and a consistent approach to working with data and documents.

The UJICS shall operate on the basis of unified infrastructure shared by all its components. This infrastructure shall provide standardised approaches to deployment, operation, scaling and monitoring, as well as the implementation of information security requirements. Such infrastructure shall serve as the technological foundation for the stable operation and further development of the UJICS.

4 REQUIREMENTS FOR THE INFORMATISATION TOOL

4.1 Requirements for the Structure and Operation of the Informatization Tool

The functional architecture has been developed on the basis of the UJICS Concept. It is not limited to that Concept and may be refined during implementation.

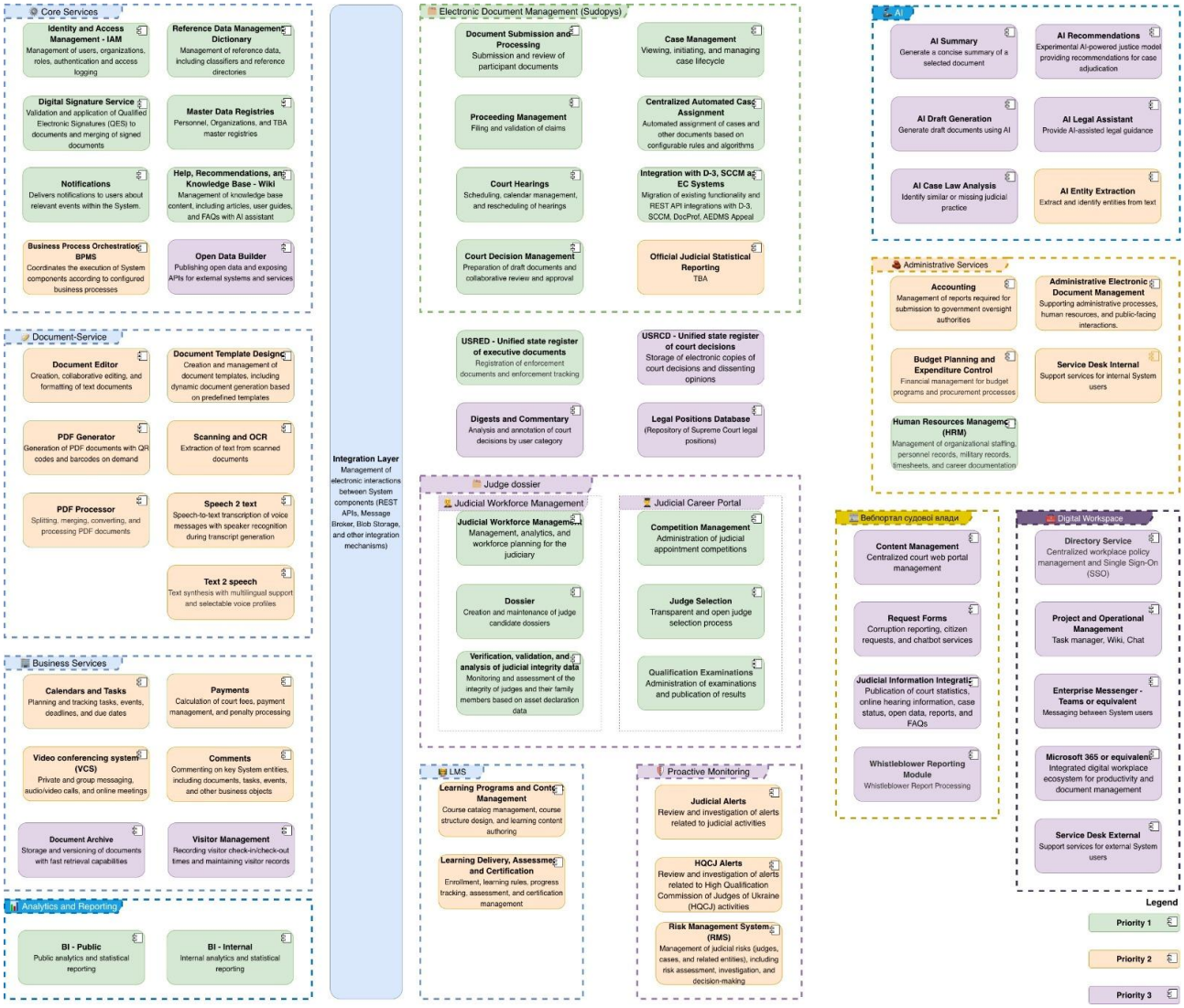

Figure – Functional Architecture of the System

4.2 Requirements for the Functions Performed by the Informatization Tool

The key functions of the System components to be covered by the development under this document are as follows:

1. Core services shall form the common technological platform, or core, of the System and shall provide the following functions:

1.1. Identity and Access Management (IAM): centralised user registration, configuration of roles and access rights and user identification, authentication and authorisation, with comprehensive activity logging.

1.2. Reference Data and Classifiers: creation and maintenance of common classifiers, System reference directories and Master Registers in order to ensure data integrity across all subsystems.

1.3. Cryptographic service: ensuring the legal validity of documents through mechanisms for applying and verifying qualified electronic signatures, as well as processing signed data packages.

1.4. Notification service: timely notification of users of System events, business-process events and tasks through internal and external communication channels.

1.5. Help and Guidance, Knowledge Base - Wiki: maintenance of electronic documentation, instructions and answers to frequently asked questions, including Wiki and FAQ materials, in order to assist users in real time.

1.6. Master Registers Service: registration and maintenance of core UJICS records and entities, including judicial authorities and bodies, organisational units and positions, legal entities/private entrepreneurs, natural persons, representatives, employees of judicial authorities, judges and other relevant entities.

1.7. Unified Personal User Environment: a toolset for creating and managing interface elements within the User Cabinet.

A UNIFIED INFRASTRUCTURE shared by UJICS components, which shall provide standardised approaches to deployment, operation, scaling, monitoring and information security.

4.3 Main Business Processes

ACCESS MANAGEMENT

Identity and Access Management, hereinafter ‘IAM’, shall support the business processes of centralised registration and management of groups and users, assignment of roles and access rights in accordance with mandates, user authentication and authorisation when accessing System services and access lifecycle management, including the granting, amendment and revocation of rights. The service shall also implement business processes for recording authentication, authorisation and access events, followed by their transmission to the centralised logging service in order to support control measures and information security.

REFERENCE DATA AND SHARED SERVICES

Reference data and shared services shall support the business processes for the creation, maintenance, updating and provision of standardised reference and master data for use by all System services. They shall also support the reuse of standard functionality, including the signing of electronic objects, dispatch of system messages and notifications and exchange of data between System components and external information systems. Implementation of these processes shall ensure data consistency, reduce duplication of functionality and improve the efficiency of supporting user business processes within the System.

4.4 Description of System User Roles and Access

The role model may include both end-user roles focused on the processing of information and roles with enhanced privileges intended for System administration, support and security.

The role model set out below is an example of the conceptual allocation of roles within the System. It may be used as a basis, with the possibility of amendments and/or additions, for the further specification of access rights, configuration of roles and adaptation of those roles to the organisational structure and needs of System users. This is a meta-model and does not limit the range of roles available within individual subsystems.

Alias	Title	Description

P1 admin_users	User Administrator	A role responsible for maintaining and updating user accounts in the System, assigning and amending roles and access rights in accordance with mandates and monitoring the correctness of users' access to UJICS functionality and data. Within this role, the User Administrator shall create, update, block and deactivate accounts and support the lifecycle of user access. The System shall enable management of administrator permissions in order to permit configuration of administrative access
P2 admin_organisations	Organisation Administrator	A role responsible for maintaining, updating and controlling organisation data in the System, including the creation, updating and deactivation of organisation records and management of their structure and core attributes. Within this role, the Organisation Administrator shall ensure the accuracy and integrity of organisational data and the use of standardised reference directories

4.4.1 Roles and Access Rights

The System shall manage user access to functions and data on the basis of two principal approaches:

- role-based access control
- attribute-based access control.

The System shall be sufficiently flexible to enable the addition of other access-control methods in the future where required. It shall be possible to connect and/or modify access control for each individual subsystem where necessary.

As the principal access-control models for users and other systems, the Contractor shall use Role-Based Access Control, RBAC and Attribute-Based Access Control, ABAC, in order to segregate users' rights of access to UJICS objects.

The access-management functionality shall also enable the implementation of additional access-control models required for other subsystems.

The list of roles and the set of access rights assigned to each role are conceptual and may be further specified and supplemented during the development of the Technical Specification, taking account of the requirements of the System Owner, the specific features of business processes and regulatory restrictions. The final set of roles and corresponding access rights shall be determined and described in the Technical Specification.

Access rights shall determine whether a user may perform a particular action within the System, as follows:

✓ — access is granted;
✓ + context — access is granted subject to the specified context;
absence of information — access is not granted.

Entity	Function	User Administrator	Organisation User Administrator	Organisation Administrator
Users	View the user register	✓ (all users)	✓ (users of the relevant organisation)	
	View a user record	✓	✓ (users of the relevant organisation)	
	Create a user	✓	✓ (users of the relevant organisation)	

	Edit a user record	✓	✓ (users of the relevant organisation)	
	Deactivate a user	✓	✓ (users of the relevant organisation)	
	Reset a password	✓	✓ (users of the relevant organisation)	✓
Organisations	View the organisation register	✓		✓
	View an organisation record	✓		✓
	Create an organisation			✓
	Edit an organisation record			✓

The list of roles shall not be limited to IAM roles and may include subsystem roles registered in IAM. The titles and sets of entities, functions and roles are preliminary and may be refined during the development of the System.

5 FUNCTIONAL REQUIREMENTS

5.1 Access Management — Identity and Access Management (IAM)

The purpose of IAM is to provide centralised user authentication and management of users, roles, access rights, sessions and action audits within the UJICS. The service shall also support mechanisms for data population and data exchange with existing subsystems.

Figure: User and Organisation Management Use-Case Diagram

1. Authentication and Session Management

1.1. The System shall provide centralised user identification, authentication and authorisation within the UJICS through the IAM service.

1.2. The System shall support authentication using:

1.2.1. a username and password, for non-residents;

1.2.2. two-factor authentication, including OTP in accordance with an agreed standard or an equivalent solution, with configurable code validity periods;

1.2.3. a qualified electronic signature (QES) stored on a secure medium or in a secure cloud environment, where required by legislation and the System security policies;

1.2.4. an advanced electronic signature in file format (AES), where required by legislation and the System security policies;

1.2.5. authentication methods recognised under eIDAS;

1.2.6. BankID.

1.3. The System shall enable an authentication method to be assigned to an individual user or group of users, taking account of their legal statuses, either manually by an administrator or automatically on the basis of additional attributes to be finally determined during the development of the Technical Specification. For example, authentication using a QES stored on a secure medium may be assigned to officials of judicial authorities.

1.4. For users who do not possess a QES of a Ukrainian official or natural person, an account may be created only by a Administrator of the System.

1.5. The System shall support protection mechanisms against automated access attempts, including CAPTCHA or equivalent mechanisms.

1.6. The System shall support file-based, hardware-based and cloud-based QES solutions.

1.7. The System shall provide integration with qualified trust service providers, the BankID authentication provider and eIDAS-compatible authentication mechanisms. The Administrator shall be able to determine which subsystems and subsystem elements a user may access depending on the authentication method used.

1.8. The System shall authorise a user authenticated using a QES only after verifying:

1.8.1. certificate validity;

1.8.2. certificate validity period;

1.8.3. certificate status;

1.8.4. compliance of other certificate attributes, including affiliation with an organisation and position held.

1.9. Where QES, BankID or username-and-password authentication is unsuccessful, the System shall deny access and inform the user of the reason. It shall provide a link to help materials concerning resolution of the issue and obtaining technical support.

1.10. The System shall provide a Single Sign-On, SSO, mechanism for access to System components without repeated authentication or intermediate redirects.

1.11. The System shall provide user session management, including:

1.11.1. configuration of a limit on the number of concurrent sessions, for example up to five;

1.11.2. configuration of automatic termination of a session after a defined period of inactivity, which may be set separately for individual UJICS subsystems, modules or services;

1.11.3. limitation of the maximum active-session duration;

1.11.4. revocation of sessions;

1.11.5. forced termination of sessions by an Administrator or the security system;

1.11.6. recording of logins and concurrent login events, including logging of the IP address and device information from which a login was performed.

1.12. The System shall issue access tokens, for example JWTs, for integration with other System services.

1.13. The System shall enable access to specified entities, including documents, files, video conferencing sessions and calendar items, with the possibility of setting validity periods and single-use request parameters.

1.14. The System shall manage the lifecycle of user accounts, including their creation, activation, blocking and deactivation.

2. Support for Standard Authentication and Authorisation Protocols

2.1. The System shall support standard protocols, including OAuth 2.0 and/or OpenID Connect (OIDC), as the principal mechanism for interaction between IAM and System services, including for:
- 2.1.1. user Single Sign-On to System services;
- 2.1.2. client application access to System service APIs;
- 2.1.3. machine-to-machine interaction.

2.2. The System shall provide centralised client management, including:
- 2.2.1. client registration;
- 2.2.2. configuration of permitted redirect URIs;
- 2.2.3. restriction of permitted flows.

2.3. The System shall issue access tokens containing user identifiers and the access context required by System services to verify rights and carry out subsequent authorisation.

2.4. The System shall enable revocation, validation and limitation of access-token validity periods in accordance with System security policies through configuration, without requiring changes to source code.

3. Role Model and Identification

3.1. The System shall implement user access based on roles, RBAC, with the possibility of assigning one or more roles to a user, and on attributes, ABAC.

3.2. The System shall enable a role to be copied and subsequently edited.

3.3. The System shall support access modes determined by the user’s authentication level, including:
- 3.3.1. anonymous access;
- 3.3.2. authorised access.

3.4. IAM shall determine the access mode on the basis of authentication results and apply the relevant access-control policies.

3.5. The System shall enable the review of registered objects and the list of available system rights for each object.

3.6. The System shall support access validation based on a combination of:
- 3.6.1. user roles;
- 3.6.2. user attributes, including court, body and status;
- 3.6.3. type of requested action, including read, create, edit and approve.

3.7. The System shall provide System services with information on a user’s roles. Those roles shall be interpreted by System services as a set of permissions to view, edit or otherwise act upon information objects.

3.8. The System shall maintain a centralised UJICS role register as a set of system access-control objects.

3.9. The Contractor shall develop a tool for registering user roles and policies, and shall enable developers of other subsystems to register their local roles and policies in the core IAM service.

4. User Management

4.1. The System shall maintain a centralised IAM user list.

4.2. An Administrator shall be able to view the full list of users with filtering and search functionality.

4.3. The System shall enable registration of a new user, subject to uniqueness checks based on the Taxpayer Registration Number, the Unique Record Number in the Demographic Register, or the passport series and number.

4.4. The System shall support a user invitation process with registration confirmation.

4.5. A user shall obtain access to the System, including the User Cabinet, following successful authorisation.

4.6. An Administrator shall be able to:

4.6.1. edit user roles;
4.6.2. block and unblock a user;
4.6.3. review the user's session history.

4.7. A user shall be blocked at the level of that user's legal status. For example, a user may be blocked in the capacity of an official while retaining access as a natural person.

4.8. The System shall support a full CRUD model for the user record, including:
4.8.1. creation;
4.8.2. viewing;
4.8.3. editing;
4.8.4. deactivation.

4.9. A user record shall contain identification, attribute and organisational data required for:
4.9.1. authentication;
4.9.2. authorisation;
4.9.3. application of access policies.

4.10. The System shall support management of user attributes used for authorisation, with the possibility of updating such attributes from external sources, including reference directories and human resources systems.

4.11. The System shall enable access policies to be configured without changes to the source code of System services.

4.12. The System shall support the association of a user with an organisation where such information is used in the System's access models.

4.13. The System shall support the management of user groups, including:
4.13.1. creation, editing and deletion of groups;
4.13.2. assignment of roles to user groups;
4.13.3. automatic application of roles to users included in a group;
4.13.4. configuration of default roles for user groups;
4.13.5. review of group membership and assigned roles;
4.13.6. establishment of parent groups.

5. Delegation of Authority

5.1. The System shall support the delegation of user authority, including:
5.1.1. temporary delegation of roles or rights to another user;
5.1.2. specification of the validity period of the delegation;
5.1.3. delegation by an Administrator or by a user;
5.1.4. automatic termination of delegated rights upon expiry of the specified period;
5.1.5. audit of delegated authority;
5.1.6. multi-level delegation.

6. Security Events, Audit Trails and Logging Integration

6.1. The System shall record security events relating to:
6.1.1. User attributes, including IP address and device details;
6.1.2. authentication attempts;
6.1.3. successful and unsuccessful authentication;
6.1.4. changes to roles, attributes and access policies;
6.1.5. the blocking or unblocking of accounts.

6.2. The IAM service shall not implement centralised audit, event analytics or monitoring. It shall only generate audit events in a structured format and transmit them to the System's centralised logging and monitoring component.

7. IAM Service Notifications

The IAM service shall generate notifications for transmission through the Notification Service in relation to the following events:

7.1. user registration;
7.2. any change to user-account attributes.

The precise list of events for which user notifications shall be generated shall be determined in the Technical Specification.

8. Integration with System Services

8.1. The System shall provide other UJICS components with programmatic interaction mechanisms for:
- 8.1.1. validation of access roles;
- 8.1.2. retrieval of user identification and attribute data.

8.2. The System shall be the single point for management of access to the System, but shall not serve as a source of business data.

8.3. System services shall be able to query IAM in real time in order to validate access roles for a specific action or resource.

8.4. The System shall provide System components with a standardised user access context, including:
- 8.4.1. user identifier;
- 8.4.2. list of assigned roles;
- 8.4.3. group membership;
- 8.4.4. user attributes used in the validation procedure.

9. Organisation Information

9.1. The System shall support the maintenance of a list of organisations that may be used:
- 9.1.1. as user attributes;
- 9.1.2. as a context for authorisation and access policies.

9.2. The System shall support CRUD operations for organisations, including:
- 9.2.1. creation;
- 9.2.2. viewing;
- 9.2.3. editing;
- 9.2.4. deactivation, or soft deletion.

9.3. The System shall support the automated creation of organisations in the IAM service and updating of their data from the relevant Organisation Master Register.

10. IAM Service Authorisation Functions:

10.1. The System shall include a separate authorisation service performing the roles of a Policy Decision Point and a Policy Administration Point.

10.2. The service shall manage registers of protected objects and determine permitted actions in relation to those objects.

10.3. The service shall enable the creation and storage of access policies based on a combination of user attributes, resource attributes, roles and request context.

10.4. The service shall provide application subsystems with an interface for retrieving permissions in real time.

10.5. Functional components of the System, namely Applications, shall act as Policy Enforcement Points and shall query the service where necessary before performing operations.

10.6. Certain subsystem components may constitute fully functional off-the-shelf solutions, including the accounting subsystem, the human resources subsystem or currently operating systems, with their own comprehensive mechanisms for regulating and controlling user access to actions and resources. For such subsystems, the IAM service shall provide only the Single Sign-On function.

5.2 Core Services

5.2.1 Reference Data and Classifiers

Scope of application:
- maintenance of reference data and centralised registers;
- provision of authoritative and legally significant data to all System services, preventing duplication and data desynchronisation while abstracting the processes that generate such data.

The service shall support two types of reference directories:

- centralised dynamic reference directories, shared by all subsystems, which shall:
  - provide an administrative interface;
  - enable the addition, editing and deactivation of values;
  - support versioning;
  - be used by several subsystems or services;
- centralised static reference directories, shared by all subsystems, which shall:
  - be populated through releases;
  - not be editable by users;
  - be used by several subsystems or services.

The service shall provide:

1. a tool for creating reference directories;
2. centralised storage of reference directories;
3. CRUD operations on reference-directory records, according to the relevant directory type;
4. deactivation of records without physical deletion;
5. prevention of the editing or deletion of records already used in subsystem data;
6. maintenance of change history and versioning of reference directories;
7. support for hierarchical reference directories;
8. the ability to maintain multiple language forms, including different grammatical cases;
9. export of reference directories through an API;
10. automatic updating of reference directories through integration mechanisms, where available;
11. search, filtering and sorting;
12. auditing of changes to reference directories;
13. management of access rights to the administration of reference directories.

The exact list and content of reference directories shall be determined by each UJICS component during detailed analysis of the relevant subsystem domain and shall be specified in the Technical Specification for that subsystem. The Contractor shall take account of the expectation that each UJICS component will require, on average, between five and twenty reference directories and/or classifiers. Most reference directories are expected to be linear and use a ‘key: value’ format. However, several hierarchical reference directories are also expected, including the Classifier of Administrative-Territorial Units and Territorial Communities, KATOTTG, which is used in the methodology for forming geographical addresses. Several hierarchical faceted classifiers are also expected, including the ‘Document Type Classifier’.

5.2.2 Notification Service

The Notification Service is intended for the centralised generation, processing, delivery and storage of messages for System users through defined notification channels, on the basis of events occurring in UJICS subsystems. The service shall select and apply notification-delivery channels, including email, SMS, push notifications in supported messenger applications and internal System messages, according to the event type and usage scenario.

The service shall support editable notification templates for different types of messages. This shall enable standardisation of message content and format, ensure the correct and consistent display of messages for all users and provide centralised message delivery.

The Notification Service shall provide:

1. An event-driven notification-generation model:
   1.1. generation of notifications on the basis of events received from other subsystems and services;
   1.2. support for an integration API, including integration with external services, such as Viber, and/or a message broker for transmission of events by subsystems;
   1.3. processing of events independently of subsystem business logic.

2. Classification of notifications by type, including:

   2.1. service notifications, including technical messages, errors, updates and security events;
   2.2. user notifications;
   2.3. deadline notifications;
   2.4. notifications relating to documents or processes;
   2.5. other types determined by the System Administrator.
3. Personal notification-receipt settings:
   3.1. the ability to activate or deactivate notification types;
   3.2. selection of delivery channels for each notification type;
   3.3. configuration of time windows for receiving notifications;
   3.4. configuration of subscriptions to events or objects;
   3.5. centralised storage of user settings.
4. Centralised administration:
   4.1. definition of notification types;
   4.2. management of available delivery channels;
   4.3. configuration of message templates;
   4.4. determination of notifications whose settings shall not be available to users;
   4.5. management of message categories.
5. Storage and notification history:
   5.1. storage of generated notifications;
   5.2. storage of information on the delivery channel used;
   5.3. notification statuses, including ‘New’, ‘Read’ and ‘Processed’;
   5.4. changing notification status by the user or automatically;
   5.5. the ability to perform bulk operations on notifications;
   5.6. generation of delivery receipts;
   5.7. generation of reports on notifications sent and received, with the ability to configure display parameters through the administrative interface. The specific list of reports shall be determined in the Technical Specification.
6. Categorisation and grouping:
   6.1. differentiated processing priority for notifications on the basis of their category;
   6.2. grouping of notifications by category;
   6.3. filtering of messages by type or source.
7. Interaction with other services and subsystems:
   7.1. the service shall be used by all UJICS subsystems;
   7.2. subsystems shall determine the events and conditions under which notifications are sent;
   7.3. the service shall not contain subsystem business logic.
8. Import of existing historical data.
9. Interaction with external message-delivery providers:
   9.1. integration with the Diia mobile application for push notifications;
   9.2. delivery through official chatbots, including Viber, Telegram and WhatsApp;
   9.3. integration with SMS-delivery providers through standard interaction protocols.

5.2.3 Document Signing — Crypto Service

Within the Unified Personal User Environment, the System shall support:

- integration with the UJICS electronic identification system, hereinafter the ‘UJICS Identification Widget’;
- integration with the id.gov.ua electronic identification system, hereinafter the ‘id.gov.ua Identification Widget’;
- integration with the UJICS electronic signature system, hereinafter the ‘UJICS Signing Widget’;
- integration with the id.gov.ua electronic signature system, hereinafter the ‘id.gov.ua Signing Widget’.

The ‘Document Signing’ component, hereinafter the ‘Crypto Service’, is a System service intended to:

- verify a signed object, for example structured data or a file;

- combine signed objects and generate output in P7S format;
- sign an object.

The Crypto Service shall:

- support operation with key formats in accordance with the CMU Resolution No. 1298 of 12 December 2023 and other applicable legislative requirements;
- support currently operating qualified trust service providers in Ukraine;
- automatically identify the electronic trust service provider;
- automatically verify certificate validity, including the validity period and certificate status;
- identify and verify the signer and retrieve signer attributes from the certificate;
- enable information to be obtained on the signature type, namely an advanced electronic signature (AES) or a qualified electronic signature (QES);
- use only certified cryptographic information-protection tools that hold a valid positive expert opinion of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP);
- perform cryptographic operations only and shall not contain subsystem business logic.

The Widget shall:

- support file-based, cloud-based and hardware keys;
- enable the application of an advanced electronic signature or a qualified electronic signature without repeated upload of the key file, repeated selection of a trust service provider or repeated entry of a password during an active user session, while providing an explicit notice to the user that they are signing a digital document or file;
- support batch signing of documents.

5.2.4 Help and Guidance, Knowledge Base — Wiki

The ‘Help and Guidance’ and ‘Knowledge Base’ System components, hereinafter the ‘Wiki Service’, are intended to manage knowledge and support users through the centralised accumulation, structuring, updating and provision of knowledge concerning System operation, functional capabilities, business processes and rules for use.

The Wiki Service shall be a shared functional capability used by all System components to:

- provide reference information;
- support users while they work with the System.

The Wiki Service shall not replace support services and shall not perform incident-management or request-management functions.

1. General Principles of Knowledge Management
   1.1. The service shall provide for the centralised accumulation, storage and provision of knowledge for System users through a single repository of instructional, reference and methodological materials.
   1.2. The service shall serve as a single point of access to knowledge concerning:
      1.2.1. use of System functionality;
      1.2.2. performance of procedural and official actions;
      1.2.3. methodological guidance and procedures.
   1.3. The service shall not contain the business logic of other System services. It shall perform a supporting information and reference function.
2. Content Types and Knowledge Consolidation
   2.1. The service shall support the storage and publication of the following content types:
      2.1.1. Knowledge Base articles;
      2.1.2. frequently asked questions, FAQs, with the ability to structure them by topic and category;
      2.1.3. regulatory and legal materials, organisational and administrative materials, information on professional practice and other relevant materials;

2.1.4. instructions and procedures in PDF and HTML formats;
2.1.5. methodological guidance;
2.1.6. video instructions;
2.1.7. images, diagrams and screenshots.

2.2. The service shall ensure storage of unstructured content, namely files, in external object storage without storing binary content directly in the subsystem database.

2.3. The service shall ensure logical consolidation of all content types within a single Knowledge Base information environment, irrespective of format.

2.4. The service shall support categorisation of Knowledge Base materials by category, topic and tag, with the ability to use them for navigation, filtering and search.

3. Content Lifecycle Management

3.1. A user with the relevant access rights shall be able to create, edit and delete Knowledge Base articles.

3.2. The service shall support an article lifecycle that may include the following states:

3.2.1. Draft;
3.2.2. Pending Approval;
3.2.3. Published;
3.2.4. Archived.

3.3. Where an article is in the ‘Draft’ or ‘Pending Approval’ state, it shall not be available to end users.

3.4. The service shall support article versioning, including the ability to:

3.4.1. view change history;
3.4.2. compare versions;
3.4.3. restore a previous version without loss of history.

3.5. The service shall enable instructions to be updated without loss of access to previous versions. This shall be critical where legislation or procedures change.

3.6. The service shall retain information on the author of changes, the person who approved the relevant material and the date on which Knowledge Base materials were updated.

4. Knowledge Search and Indexing

4.1. The service shall provide search functionality within the Knowledge Base, including search by:

4.1.1. article title;
4.1.2. article text.

4.2. A user shall be able to search for information using keywords, phrases and synonyms.

4.3. Search results shall take account of the user’s access rights determined by the IAM service.

5. Contextual Help and Guidance (Context Engine)

5.1. The service shall provide contextual help and guidance to the user on the basis of:

5.1.1. the System page on which the user is located;
5.1.2. the action being performed by the user;
5.1.3. the user’s role.

5.2. Where a user is on a particular page or performs a specified action, the System shall automatically propose relevant articles or instructions.

5.3. The module shall include a mechanism for matching interface context, including URL, screen identifier or action identifier, with relevant Knowledge Base materials.

5.4. Subsystems shall be able to determine the relationship between interface elements and Help materials through the Wiki Service API.

6. Segregation of Access to Content

6.1. The service shall segregate access to content in accordance with the user’s role.

6.2. Where a user does not have access rights to particular material, that material:

6.2.1. shall not be displayed in search results;
6.2.2. shall not be accessible through a direct link.

6.3. The service shall use the centralised UJICS IAM service and shall not implement its own authentication system.

7. Feedback and Analytics

7.1. A user shall be able to assess the usefulness of an article, for example by selecting ‘Helpful’ or ‘Not helpful’.

7.2. The service shall retain content-usage statistics, including:

7.2.1. views;
7.2.2. search queries;
7.2.3. user ratings.

8. Notifications and Knowledge Updating
8.1. The System shall initiate notifications to subscribed users where critical instructions or methodological materials are updated.
8.2. Notifications shall be transmitted through the System's centralised Notification Service.

9. User Interface
9.1. The service shall provide a floating Help widget accessible from any System screen.
9.2. The service shall provide a separate Knowledge Base portal with:
9.2.1. a category tree;
9.2.2. search functionality;
9.2.3. content filtering.
9.3. A user shall be able to export Knowledge Base materials, or parts thereof, in PDF format or print them.

5.2.5 Master Register Service

The Master Registers Service is intended for the centralised storage and management of the core UJICS records and entities. Master Registers shall constitute the Source of Truth for other subsystems.

The service shall provide:

- creation of record cards for objects and entities of record shared by UJICS components;
- unambiguous identification of objects and entities of record across all UJICS components;
- recording of changes to each object or entity of record shared by UJICS components, in order to preserve its lifecycle history;
- a standardised integration model;
- segregation of access;
- logical relationships between Master Registers.

The service shall not constitute a set of electronic registers within the meaning of the Law of Ukraine 'On Public Electronic Registers'. Information contained in the service shall be used for the internal needs of the UJICS.

Data may be entered into and viewed in Master Registers through their own front ends, including those for organisational structure and natural persons, or through use as back-end services by other subsystems or services with API access, or by means of defined internal interaction mechanisms.

The business logic governing the creation and amendment of records shall be defined in the Technical Specification and shall not contradict applicable regulatory and legal acts.

The System shall enable implementation of core Data Governance principles, including identification of authoritative data sources, control of data quality, uniqueness and consistency and tracking of changes. The Data Governance Policy shall be provided by the Technical Administrator and shall comply with the current requirements of the UJICS.

The System shall enable the exercise of data-subject rights, including access, rectification, restriction of processing and erasure, determination of data-retention periods and auditing of operations involving personal data, in accordance with the requirements of Ukrainian legislation.

Main Functional Requirements. The service shall:

1. enable the creation, viewing and updating of record cards in accordance with defined business logic;
2. maintain a single unique identifier for each entity;

3. ensure lifecycle history of changes, namely an audit-traceable state history;
4. support integration with:
   4.1. the Human Resources System;
   4.2. the ‘Electronic Interaction’ component;
   4.3. the ‘Judicial Dossiers’ subsystem;
5. enable other UJICS subsystems to integrate with the Master Registers Service and determine the set of attributes available to each subsystem;
6. ensure segregation of access to complete lists of records;
7. enable records to be searched by identifier or attribute;
8. support relationships between Master Registers through a single identifier;
9. provide a Golden Record mechanism for specified entities;
10. support versioning of the organisational structure.

Main Master Registers (the list of Master Registers below may be refined during preparation of the Technical Specification):

Register	Purpose
Natural persons	This Master Register shall constitute the central record-management core of the UJICS and shall cover all natural persons who are referred to or involved in judicial-system processes in any manner, irrespective of whether they are System users. The register shall include: • persons participating in proceedings, including claimants, defendants and applicants; • judges; • employees of judicial authorities; • candidates for positions; • representatives of parties; • persons mentioned in documents; • other natural persons associated with justice-sector processes. The Master Register shall operate on the basis of a single natural-person identifier used to establish links with all other Master Registers and subsystems. Sources of creation: • self-registration by a natural person upon first login, with future validation against and/or retrieval of data from State registers; • initial data loading from the Human Resources System, after which the Human Resources System shall become a data consumer; • creation of a Natural Person record card where there is a need to refer to that natural person in documents generated by the System. The register shall provide: • a limited front-end interface for searching for and viewing a specific record card; • no ability to view the complete list of natural persons; • accumulation of data throughout the lifecycle; • definition of data-population business logic at the Technical Specification stage; • a legally reliable model for data changes in accordance with regulatory and legal acts.
Photographs of Natural Persons	This shall be a specialised Master Register for storing photographs of natural persons associated with records in the Natural Persons Master Register. The register shall provide:

Register	Purpose
	• storage and versioning of photographs; • linkage to the single identifier of a natural person; • use in identification services, profile visualisation and personnel records management; • compliance with personal-data-protection requirements. Sources: • the Human Resources System; • self-registration; • integration processes.
Advocate profiles	This shall contain a specialised information block concerning a natural person in their capacity as an advocate. It shall be created as a result of the self-registration business process through the Electronic Cabinet, with data validation against the Unified Register of Advocates of Ukraine. Characteristics: • it shall not contain personal data, as it shall use a reference to the Natural Persons Master Register; • information shall be static and independent of a specific case; • it shall provide the minimum necessary dataset for interaction between subsystems; • an advocate may be a member of an advocates' association; • a record shall be created only after confirmation of advocate status. The aggregate of these records shall form the complete list of advocates interacting with the UJICS.
Judge profiles	This shall contain an information block concerning a natural person in their capacity as a judge, irrespective of: • current place of work; • current judicial office, retirement or holding an administrative judicial office. The Master Register shall contain the minimum necessary dataset for the operation of other services. Detailed information shall be maintained in the 'Judges' Dossiers' subsystem. The register shall provide: • viewing of the complete list of judges, subject to access rights; • linkage to the Natural Persons Master Register; • use in automated allocation, analytics, personnel records management and all other System functions requiring a list of all natural persons who have ever held, or currently hold, a judicial position.
Profiles of Judicial Candidates	This register shall be created as a result of processes performed by the 'Judges' Dossiers' subsystem. It shall contain: • its own status model, including competition participant, winner and recommended candidate; • linkage to the Natural Persons Master Register. It shall reflect the results of processes without storing their detailed logic, which shall remain in the dedicated subsystem, namely the 'Judges' Dossiers' subsystem.
Profiles of Jurors, Insolvency Practitioners, State and	These profiles shall be created according to logic similar to that used for advocate, judge or judicial-candidate profiles.

Register	Purpose
Private Enforcement Officers, Forensic Experts, Notaries and Prosecutors	Confirmation that the relevant status has been granted shall take place in accordance with the applicable legal procedures. These profiles shall be intended for the centralised record management of specialised procedural statuses of natural persons required for the operation of specific subsystems. The list of such profiles may be refined during preparation of the Technical Specification, depending on the business needs of the relevant specialised subsystems.
Legal Entity / Private Entrepreneur	This shall be a unified Master Register combining legal entities and sole proprietors as procedural entities participating in judicial-system processes. The Master Register shall contain: • registration data from the Unified State Register; • entity type, namely legal entity or sole proprietor; • core identification and registration attributes; • relationships with representatives. Legal entities and sole proprietors shall not be direct UJICS users. Actions on their behalf shall be carried out by authorised natural persons. Record creation: • self-registration through the Electronic Cabinet; • validation against and/or retrieval of data from the Unified State Register.
Authorised Representatives of a Legal Entity / Private Entrepreneur or Natural Person	This shall contain representation record cards recording: • the representative, being a natural person; • the represented person, being a natural person, legal entity or sole proprietor; • the legal basis for representation; • the period of validity of authority. Characteristics: • a representative shall always be a specific natural person; • advocates shall be required to have a registered Electronic Cabinet; • the register shall not have its own fully functional front end, and data shall be entered and viewed through the User Profile in the Electronic Cabinet; • the complete list of records shall not be available to users in any role; • a search mechanism shall be provided to verify authority.
Contact details	This shall be an operational Master Register for the standardised storage of contact information relating to: • natural persons; • organisations; • organisational units. The register shall provide: • centralised management of contact details; • reuse across different subsystems; • integration with the Human Resources System and the User Profile.
Bank details	This shall contain a centralised data block relating to the bank details of: • natural persons; • legal entities / private entrepreneurs; • judicial authorities. Sources: • the Human Resources System;

Register	Purpose
	• self-registration. The register shall be used by financial and procedural services.
Judicial Authorities, Judicial Self-Government Bodies, Advisory and Consultative Bodies of Judicial Authorities, State Authorities and Local Self-Government Bodies	This shall constitute the centralised Golden Record of the organisational structure. It shall include: • organisation record cards; • organisational-unit record cards; • position record cards. Organisation: • may be a legal entity or an entity without legal personality; • shall retain historical data; • shall be created by the Technical Administrator or authorised persons; • may be imported from the Human Resources System; • shall be enriched with data from the USR. Organisational unit: • shall reflect the staffing structure; • shall integrate with the personnel records subsystem. Position: • shall meet the needs of two record-management areas: 1) the staff establishment for standard personnel records purposes, and 2) records of judicial positions for the purposes of processes of the HQCJ; • shall contain statuses from the Human Resources System and statuses generated through processes of the HQCJ; • shall maintain historical records as instances of standard positions in specific bodies and shall answer the question: 'Which position existed in which body and during what period?' The Master Register shall support historical data, status management and versioning. It shall have a complex role-based interface. In addition to bodies and organisations that are legal entities, the register shall support register operations involving entities without legal personality. The list of such organisations shall be determined in the Regulation on the UJICS.
Employees and Other Staff of Judicial Authorities	This shall contain record cards of employees, including civil servants and other staff. The register shall be populated from the Human Resources System. It shall provide: • linkage between a natural person and a position; • use in other services.
Judges Holding Office	This shall be a specialised Master Register of active judges holding positions in judicial authorities. It shall differ from the Employees and Other Staff Master Register through: • an expanded set of attributes; • different access levels; • mandatory linkage to the Judge Profile; • specific record-creation logic. It shall constitute the golden record for services requiring an up-to-date list of judges, including automated allocation.

5.3 Unified Personal User Environment

5.3.1 General Description

The System User Cabinet shall constitute the Unified Personal User Environment. It shall provide a consistent user experience (UX) and serve as a container for rendering the functional interfaces of System components. The User Cabinet shall not contain business logic specific to individual System components. It shall be responsible for navigation and visual consistency.

In accordance with the Concept, the System User Cabinet shall communicate consistent approaches to work organisation and foster a shared internal culture through common styles, graphic elements, the Unified Personal User Environment and standardised processes, templates, reference directories and classifiers.

5.3.2 Main Functional Requirements

1. The User Cabinet shall dynamically load System components. Any change to or update of the interface of one System component shall not require rebuilding the entire User Cabinet.
2. The User Cabinet shall enable pages to be opened in a new tab.
3. The User Cabinet shall manage common interface elements in accordance with the UX/UI design, including:
    - a global navigation menu, namely a side bar and/or top bar, with the ability to hide the side bar on smaller screens;
    - a standardised header, including the User Profile, role selection and notifications;
    - a standardised footer;
    - a standardised favicon for each System component and the title of the active web page. For example, for the IAM service: Sign in — 🔑 IAM | UJICS; Users — 🔑 IAM | UJICS; First Name Surname — 🔑 IAM | UJICS;
    - a common status bar for displaying critical System statuses;
    - Help-access elements, for example a ‘Help’ button or relevant widget, enabling the opening of Wiki Service materials relevant to the user’s current context;
    - standardised interactive tooltips for interface elements in accordance with the UX/UI design;
    - other interface elements specified in the approved design.

4. The User Cabinet shall provide:
    - the ability to save individual interface settings for each user, including the order and visibility of columns in tables, the state of collapsed menus and selected dashboard widgets, as well as equivalent settings for each standard interface element for which a shared interface component is developed;
    - centralised storage of settings and their retrieval upon login from any device through the user account;
    - a standardised mechanism for user confirmation of critical actions through warning messages or dialog boxes, with clear guidance on how to address the relevant issue, in accordance with the UX/UI design;
    - display of messages to the user, including information messages, error messages, warnings and operation-progress messages, with recommendations for further action.

5. For UJICS subsystems that constitute fully functional software suites and are supplied with their own interfaces, including the Human Resources Subsystem or the Accounting Subsystem, development of an interface within the Unified Personal User Environment shall not be mandatory. However, where a user selects the relevant navigation element in the System User Cabinet interface, the User Cabinet shall redirect that user to the dedicated interface of the relevant subsystem.

6. All System interface components shall be designed in accordance with the most recent version of the Web Content Accessibility Guidelines (WCAG) applicable at the time of implementation.

5.3.3 Integration and Use Requirements

Development and Maintenance of the Design System (UI Kit)
1. Before development of the UI component library begins, the Contractor shall develop and submit to the System Owner a clickable prototype of the core interfaces and UI components for approval of the user interaction concept and visual design.
The clickable prototype shall:
   1.1. reflect the main user interaction scenarios;
   1.2. demonstrate the behaviour of key UI components;
   1.3. show the navigation and interface structure;
   1.4. be approved by the System Owner before implementation of the UI component library begins.
2. The Contractor shall develop and publish a UI component library as an npm package or equivalent and shall provide the relevant documentation.
3. Before development begins, the Contractor shall prepare and obtain approval for a clickable prototype that takes account of the design-system requirements.
4. The library shall include grids, typography, buttons, forms, tables supporting customisation features such as sorting and filtering, modal windows and other interface elements specified in the approved design.

5.3.4 User Profile in the Unified Personal User Environment

The System shall enable users to view their own User Profile within the Unified Personal User Environment and shall provide the following functionality in that profile:

1. The System shall enable users independently to manage their accounts within permitted limits, including changing a password, changing a verified email address and managing authentication factors.
2. The System shall enable users to view their current legal status and switch between available legal statuses retrieved from the core IAM service.
3. The System shall enable users to monitor login activity relating to their own accounts by viewing login logs from the centralised logging subsystem for a specified period.
4. The System shall enable specialised sections to be added to the User Profile in the User Cabinet. Such sections shall be managed by specified System components in order to display personal information relating exclusively to the relevant user.
5. For example, the ‘Personal Details’ section may be populated and managed by the ‘Register of Natural Persons Registered in the UJICS’ Master Register.

6. NON-FUNCTIONAL REQUIREMENTS

The System architecture and non-functional requirements shall prevent vendor lock-in to a particular cloud or infrastructure service provider.

All System components shall be deployable within the System Owner's own infrastructure or the infrastructure of any service provider without changes to application logic.

The use of proprietary managed services shall not be permitted where such services:

- do not have functionally equivalent self-hosted implementations;
- require the use of provider-specific APIs, SDKs or management mechanisms;
- make migration of the System to an alternative infrastructure environment impossible or substantially more difficult.

This restriction shall not apply to the use of standard protocols, open APIs and generally accepted industry standards that are independent of a particular provider.

Scaling, recovery and lifecycle-management mechanisms shall be implemented at the orchestration or infrastructure layer, rather than through proprietary services of a provider.

6.1 Requirements for the Number and Qualifications of Personnel Involved in System Operation and Support

The System shall be operated by personnel of the System Administrator and/or an authorised organisation in accordance with these Technical Requirements and the applicable regulatory and legal acts of Ukraine.

The Contractor shall propose and agree with the System Administrator the minimum capacity required for the roles listed below, without limitation thereto, to ensure the normal operation and support of the Informatization Tool, using the following format:

Functional Requirements for Personnel	Capacity (person-months)
Project and Programme Management Specialist, Product Manager	
Automation Process Analyst, Business Analyst	
Software Development and Testing Specialist, Developer	
Software Development and Testing Specialist, QA Engineer	
New Technology Implementation Engineer, Support Engineer	
IT Designer, UX/UI Designer	
Integration Engineer, DevOps Engineer	

Detailed qualification requirements for personnel responsible for ensuring normal operation of the Informatization Tool shall be determined in the Technical Specification on the basis of the selected technological solutions.

6.2 Security Requirements

The Production (PROD) environment and the Non-Production (NON-PROD) environment shall be segregated. The names of objects in different environments shall use prefixes or suffixes that unambiguously identify the environment to which the object belongs.

The System shall comply with current international information security standards, including NIST SP 800-63B and NIST SP 800-53.

For the early detection of vulnerabilities in programme code, developers shall use Static Application Security Testing, SAST and Dynamic Application Security Testing, DAST, tools provided by the System Owner during the development stage.

The System shall include protection mechanisms against the most common types of attack identified in the OWASP Top 10.

Information contained in error messages made available to external parties in relation to System components shall not disclose technical details concerning the composition or versions of such components.

The following rules shall apply at the physical layer:

1. Physical access to equipment shall be restricted and all actions shall be recorded.
2. Physical access to System backups shall be restricted in accordance with the System administration procedure and all actions shall be recorded.
3. The System shall include functionality to limit the number of requests made to the System in order to protect it against overload.
4. The System shall successfully undergo vulnerability testing using a tool provided by the System Owner in the following modes, where available:
    4.1. without an authenticated User;
    4.2. with an authenticated User.

Following such testing, a test protocol and a report confirming the absence and/or presence of vulnerabilities shall be prepared. Where critical vulnerabilities are identified, namely vulnerabilities classified as High severity or above, the Contractor shall provide an explanation, an action plan and implement measures to remediate or mitigate the impact of the identified System vulnerabilities. Following implementation of remediation or mitigation measures, the System shall contain no vulnerabilities classified as High severity or above.

Standard secure-configuration templates and ready-to-use images shall be created for the deployment of operating systems, equipment, software and additional services necessary for the normal operation of the System.

The infrastructure platform shall ensure logical isolation of System components from other services operating within the infrastructure.

For the purposes of enabling administrators and users to work with the System, standard role models for end administrators and System users shall be established and used. These shall include personalised interfaces and defined sets of operations in accordance with the roles and mandates of administrators and users. The set of permitted operations and accessible objects within an individual role shall be determined in accordance with the following information security principles: ‘need to know’ — a subject shall be granted access only to the information required to perform their tasks; ‘need to use’ — a subject shall be granted access to the information technology infrastructure only where there is a clearly defined need to do so.

The System shall provide user authentication based on a username and password, a multi-factor authentication code, optionally and mandatorily for a defined category of users such as Organisation Administrators and User Administrators, or through a QES. The System shall process only confidential information within the classification level established by Article 21 of the Law of Ukraine ‘On Information’. In accordance with paragraph 5.1, ‘Comprehensive Information Protection System’, of the UJICS Concept, information classified as ‘For Official Use’ or ‘Secret’ shall not be processed in the System. Responsibility for preventing such information from being entered into the System shall rest with users, who shall be properly instructed.

The System may support interaction with official services that provide information on IP addresses and with its own local IP address databases. It shall enable configuration of notifications

to administrators of address zones concerning the identified zone from which access to the System is made.

6.3 Ergonomic and Technical Aesthetic Requirements

End users shall access the System through the website, which forms part of the System interface. The website shall provide publicly available information and include a link to the Cabinet of registered users. For each user group, a separate User Cabinet interface shall be automatically assembled on the basis of assigned roles. The interface shall be adapted to the relevant maximum set of functions. The interfaces shall be sufficiently universal to support different functionality and enable the future expansion of the list of functions available to users.

The System shall provide users with flexible mechanisms for personalising its interface. It shall allow users to configure functionality to meet their specific and changing needs without requiring recourse to software developers. Detailed requirements for such mechanisms shall be specified in the Technical Specification.

Website design prototypes shall constitute schematic representations of layouts and individual page elements. The proportions of design elements, font and heading sizes, spacing between elements, element design and placement shall be indicative and may differ in the final implementation of the System.

The web interface shall be capable of being launched and operated using the most recent version, available at the time of System testing, of Microsoft Edge, Safari or Google Chrome. All website pages shall be displayed in the same user-friendly form on desktop computers and users' mobile devices, including tablets, laptops and smartphones, irrespective of device type and without the use of a separate mobile version. The interface shall therefore be responsive. This technology may be applied to specific functionality at the level of each subsystem, as determined in the Technical Specification.

System web components shall be accessible without the installation of additional software, including plugins, extensions or desktop software, except for software required to enable QES signing.

6.4 Information Protection Requirements

Protection of information processed by the System shall be ensured through the establishment, updating and operation of an Information Protection System, hereinafter the 'IPS', by one of the following means:

- creation of the System using basic and target security profiles, where the selection of protection measures complies with the requirements of Normative Document on Technical Protection of Information (ND TZI) 3.6-006-24, which is a translation of the NIST Cybersecurity Framework, hereinafter the 'security profile'; or
- implementation of an information security management system in accordance with the requirements of Ukraine's national information security standard DSTU ISO/IEC 27001:2023, 'Information security, cybersecurity and privacy protection — Information security management systems — Requirements', adopted by Order No. 210 of 17 August 2023 of the State Enterprise 'Ukrainian Research and Training Centre for Standardisation, Certification and Quality'.

The purpose of establishing the IPS shall be to ensure the confidentiality, integrity, observability and availability, within the scope of assigned mandates, of information circulating within the System.

The final IPS requirements shall form part of a separate Technical Specification for the establishment of the IPS for the System.

The infrastructure on which the System shall operate shall provide, at a minimum:

- detection and blocking of cyberattacks and unauthorised network activity;
- filtering and analysis of network traffic by protocol, port and sender and recipient IP address;
- protection of software against external threats, internal unauthorised access, malicious software and cyberattacks;
- termination of connections with attacking nodes when an attempted attack is detected;
- logging and recording of events relevant to cybersecurity.

6.5 Requirements for Standardisation and Unification

The System shall ensure the standardisation and unification of functions through the use of modern software tools that support a common technology for the design, development and maintenance of functional, information and software components.

The System architecture shall be based on standardised principles for the design and implementation of software components, shall follow a single architectural approach throughout the project and adhere to project-wide agreed design patterns.

The System and all software components shall comply with applicable international agreements, national regulatory and legal acts and standards in the IT field.

The System shall support data and interoperability standards, including the processing and storage of data using ASCII and Unicode (UTF-8) encodings, ensuring correct operation with text in different languages and character sets.

The preparation of documentation for the software development phase shall apply the international standards for the creation and development of informatization tools established by the Mandatory Requirements for the Creation (Modernisation, Modification and Development), Administration and Ensuring the Operation of an Informatization Tool, approved by Resolution of the Cabinet of Ministers of Ukraine No. 205 of 21 February 2025.

6.6 Requirements for the Reliability of the Informatization Tool and the Preservation of Information

System reliability shall be ensured through the stable operation of its components, preservation of data integrity and availability and minimal need for intervention by a System Administrator to restore operability. The implemented System shall ensure continuous availability of all services on a 24/7 basis, except where planned preventive maintenance or software updates are being performed, of which System users shall be notified in advance.

System fault tolerance shall be ensured automatically. Minimal Administrator intervention shall be required in responding to and remedying the consequences of component failures. Data preservation shall be ensured through software and hardware means.

The System and its components shall be equipped with data and configuration backup facilities that enable prompt restoration of operation in the event of faults, failures or emergency situations, including:

- continued System operation in the event of a failure or breakdown of any single software or hardware component;
- preservation of information at the time of a failure or breakdown of any System component, regardless of its purpose, followed by recovery after repair and restoration work;
- backup of critical System components and data, configurations and settings;
- archiving of System data and settings on a scheduled and as-needed basis, as well as restoration of data from backups.

Backups shall be performed at a frequency that ensures complete preservation and recovery of data in accordance with the approved backup schedule.

Data preservation shall be ensured in the event of:

- power failure;
- failure of information-processing equipment;
- software errors, failures or corruption.

Preservation of information processed by System components shall be guaranteed in full and data loss shall not be permitted. The System shall guarantee data integrity in the event of failures or errors through appropriate software and hardware measures, including backup, replication and transactionality mechanisms. Reliability shall be ensured through:

- comprehensive testing;
- systematic backup and archival storage of information;
- software and hardware protection against unauthorised third-party software and hardware interference;
- archival preservation of information;
- the ability to scale horizontally in real time without interruption of service;
- the ability to create cold backups of all components while ensuring data integrity and enabling all System components to be deployed from cold backups in an integrated and operable state;
- a Recovery Time Objective, RTO, of no more than two hours, being the maximum time for restoring operability of all System components, provided that the server infrastructure is available;
- System availability of not less than 99.5%, excluding planned downtime and unavailability of the primary and backup server capacity and communications facilities;
- prompt replacement of failed software and hardware facilities;
- compatibility of technical facilities and software.

All functional System components shall have redundancy of at least N+1 in order to enable maintenance and software updates of individual components without disrupting the operation of the System as a whole. This means that each key component shall have at least one standby node and, where the primary node fails, the System shall automatically switch to the standby node.

The System shall ensure observability, including logging and event auditing, in relation to all operations and events and comprehensive monitoring of System operation, including backup and recovery.

The System shall provide geographical distribution across data centres.

6.7 Requirements for Communication Methods and Facilities for Information Exchange Between Informatization Tool Components

The software shall support different types of communication channels, including mobile networks, channels with limited bandwidth and high latency and intermittently connected networks.

The software shall be designed to operate with a minimum user Internet connection speed of 1 Mbps. Detailed requirements for each subsystem shall be determined in the Technical Specification.

6.8 Requirements for Operating Environments of the Informatization Tool

For the purposes of ensuring conditions for development and operation, the System shall be deployed across the separate environments set out in the table below.

Type	Environment	Description
PROD	PROD	The Production environment shall be used to process real data.
NON-PROD	STAGE	An environment that replicates the Production environment in terms of configuration and functionality. It shall be used for acceptance testing and incident reproduction.
	QA	An environment for testing developed functionality and resolved defects before deliverables are transferred to STAGE for acceptance testing.
	DEV	An environment for development and testing of functional prototypes. It shall be used by developers for intermediate testing of new functionality.

Initial deployment of the DEV, QA and STAGE environments shall be performed by the Contractor using the resources of the System Administrator. Deployment of the PROD environment and its subsequent administration shall be performed by the System Administrator. The Contractor shall administer the DEV, QA and STAGE environments throughout the development period. All costs related to the deployment, operation and administration of the DEV, QA and STAGE environments shall be borne by the Contractor.

6.9 Requirements for System Development and Modernisation Capability

The System shall be capable of further development and modernisation in-house through the use of software tools that do not require the mandatory involvement of the developer.

The System shall have capacity for further development and shall permit further modernisation, including:

- introduction of additional components or enhancement of existing components, access segregation and information protection;
- expansion of the information and telecommunications network.

The System shall provide a standard mechanism for updating versions of any third-party dependencies, including libraries, components and plugins, used in the System for at least ten years from the date the System is commissioned.

6.10. Linguistic Support Requirements

The System shall support multilingualism, i18n/l10n, for the interface, messages and reference directories. Ukrainian, uk-UA and English shall be supported as mandatory languages in accordance with IETF BCP 47, with the possibility of expanding the list of locales in the future. The list and scope of data to which multilingualism applies, including reference directories, messages and interface elements, shall be determined during development of the Technical Specification, taking account of the functional needs of subsystems and legislative requirements. Languages and translations shall be managed through the administrative interface.

6.11 System Capacity Requirements

The System capacity shall ensure the processing of requests and operations performed by users, taking account of the simultaneous operation of a significant number of users and possible growth in workload. The System architecture shall be designed for peak loads, including those arising during emergencies.

The System shall operate reliably under peak loads that may occur as a result of an increase in the number of concurrent users or mass automated requests. Degradation of response times under load shall be predictable.

To monitor compliance with System capacity requirements, statistics shall be collected and analysed, including operation execution times, the number of processed operations, the percentage of successful operations and infrastructure resource-utilisation statistics, including CPU, memory and network resources, under load.

The System shall be capable of processing information in accordance with the anticipated workload.

Users

No.	Indicator	Description / breakdown	2023	2024	2025
1	Total number of users	All registered users	EC 133,220 VCS 33,877	EC 157,054 VCS 38,413	EC 170,469 VCS 59,303
2	Internal users, including judges and assistants	Number	–	ASDS 23,000	ASDS 24,000
3	Unauthorised external users of the web portal, sessions	Number	Months 6-12: 22036749	37,164,155	41,030,966
4	Users of the USRCD with full access	Number	10,340	12,600	14,100

Main Entities

No.	Entity	Unit	2023	2024	2025
1	Cases	Number created	3,385,341	3,469,217	3,671,016
2	Proceedings	Number created	4,356,825	4,461,328	4,827,291
3	Court decisions	Number created	7,817,209	8,083,168	8,812,741
4	Enforcement documents	Number created	788,831	957,340	1,001,393
5	Notifications through the EC	Number created	800,000,000	950,000,000	1,100,000,000

Documents

No.	Indicator	Unit	2023	2024	2025
1	Documents	Number	62,157,453	72,106,168	77,835,858

2	Files	Number	39,825,839	91,685,911	180,910,079

Data

Parameter	Up to 1 KB	From 1 KB to 1 MB	From 1 MB to 10 MB	From 10 MB to 100 MB	Over 100 MB
Average size of attached file, bytes	2,373.682664	851,766.8753	12,786,417.97	106,999,087.2	1,673,141,004
Percentage of total number	0.01%	78.55%	17.76%	3.28%	0.40%

The System shall ensure the following information request-processing performance where the Internet speed is up to 100 Mbps and network latency does not exceed 100 ms:

- 90% of requests shall be completed within one second;
- 95% of requests shall be completed within two seconds;
- 99% of users shall successfully log in to the System on the first attempt;
- for complex requests, the acceptable processing time shall be determined with regard to the volume of data and the sequence of dependent requests.

6.12 Requirements for Licensing Conditions and Use of Third-Party Software

- Proprietary intellectual property rights in the software, namely the System, created as part of the provision of development services, including source code, documentation, databases and graphic elements, shall transfer in full to the System Owner upon signing the Acceptance and Handover Certificate for the services provided.
- The Contractor shall guarantee that the transferred System does not infringe the intellectual property rights of third parties.
- Open-source software may be used as part of the System only where the terms of the relevant licences, for example MIT, Apache 2.0 or BSD, allow the System Owner to use the System for its own purposes without payment of additional royalties and without mandatory disclosure of the System's proprietary source code, provided that this does not contradict the relevant licence type.
- The Contractor shall provide a complete list of all third-party libraries and components used in the System, indicating the type of their licences.
- Where it is necessary to use third-party commercial software as part of the System, the Contractor shall:
    - obtain prior approval from the System Owner for the list, cost and conditions for subsequent renewal of such licences;
    - include in its final proposal price the cost of those licences together with ten years of support;
    - where periodic licence payments, subscriptions, are required for System operation, the Contractor shall provide a Total Cost of Ownership, TCO, calculation covering a period of no less than three years.
- The Contractor shall transfer to the System Owner the source code of all software created under the contract, as well as settings, configuration files and deployment scripts.
- Licences for the right to use software included in the System shall be supplied in the form of licence certificates and, where necessary, licence keys or files installed together with the relevant software as part of the System.
- Licences for software used as part of the System shall be perpetual and unlimited in time.
- The supplied System software and its components shall not have End-of-Life, EOL, or End-of-Support, EOS, status.

- The licensing terms for software used as part of the System shall permit the creation, after implementation, of multiple server installations, the number of which shall be subject to agreement between the parties, for testing, development and training purposes.
- The database management system software used as part of the System shall include a free version that may be used for testing and training.
- The licence type shall allow the entire number of System users corresponding to the number of purchased licences to operate concurrently on any number of computers or virtual machines.
- Licensed software required for implementation and operation of the System shall be supplied within a timeframe sufficient to commence System implementation, configuration and commissioning services.

6.13 [QA] Development Requirements

During development, the Contractor shall be guided by generally accepted standards that are relevant to the selected programming language. The use of a specific standard shall be agreed with the System Owner during the preparation of the Technical Specification. At the request of the System Administrator, the Contractor shall provide consultations on architecture and development for up to approximately two hours per week.

The System Owner, or a technical specialist authorised by the System Owner, shall retain the right to conduct regular code reviews throughout the development period. At the request of the System Owner, the Contractor shall provide technical consultations on selected architectural solutions, methods for implementing functionality and the third-party libraries or frameworks used.

Where the review identifies deviations from generally accepted coding standards or from the Technical Specification, the Contractor shall remedy such observations within the timeframes agreed by the parties.

The Contractor shall develop and implement standardised approaches to inter-system interaction, including standardisation of APIs, data-exchange formats, error handling and versioning.

The Contractor shall ensure traceability of requirements set out in the Technical Requirements to the relevant Technical Specification, and shall define acceptance criteria and verification methods for material requirements.

6.14 [QA] Data Migration Requirements

The Contractor shall ensure the complete and correct migration of data from all required operational systems, hereinafter the ‘Data Sources’, made available by the System Administrator, namely the Electronic Court, D3, DSS, Kadry-Web, the Unified State Register of Court Decisions and VCS, to the newly created System. The migration process shall include the following stages:

- The Contractor shall conduct a comprehensive analysis of data structures and the actual data content of existing systems in order to identify discrepancies in formats, data types and logical relationships.
- During the analysis, the Contractor shall identify defects, including incomplete, incorrect or obsolete records and potential data conflicts that may arise when information from different sources is consolidated, including duplicate records and conflicting data concerning the same objects.
- On the basis of the analysis performed, the Contractor shall develop and submit to the System Administrator for approval a Data Migration Methodology.
- This document shall describe rules for correcting defects, algorithms for resolving data conflicts and the procedure to be followed where inconsistencies are identified that cannot be corrected automatically.
- The Methodology shall also describe methods for verifying and testing migration results.
- Following approval of the Methodology, the Contractor shall develop specialised software tools for automated data migration.

- The Contractor shall perform the migration and provide migration reports confirming the integrity, completeness and correctness of the data transferred to the new System.

Before migration of historical data begins, the Administrator of the System shall provide the Contractor with access to the databases used by UJICS subsystems from which data are to be transferred, descriptions of the relevant database tables, where available and shall agree the composition of data subject to migration. This shall include attributes, metadata, log records and other events to be specified at the Technical Specification stage, including but not limited to:

- information on natural persons involved in UJICS processes;
- information on natural persons as UJICS users;
- information on legal entities / private entrepreneurs participating in court cases;
- information on representatives, including advocates, of natural persons and/or legal entities / private entrepreneurs;
- information on other persons;
- information on organisations that form part of Ukraine’s judicial system and other bodies;
- reference directories.

7 TECHNOLOGY STACK

The System technology stack has been developed in accordance with the UJICS Concept, taking account of the principles of standardisation, scalability and long-term operational capability. The selection of technologies has taken account of their market adoption, maturity, active professional communities, availability of documentation and established production-use practices, as well as the ability of the System Administrator to further support, develop and maintain the System using internal or external resources.

The selected technology stack shall ensure operational continuity, reduce dependency on individual contractors and enable the further development and integration of the Informatization Tool within the UJICS without requiring fundamental changes to architectural approaches.

The Contractor may propose an alternative technology stack or individual technological components, provided that it submits substantiated justification for the proposed replacement. The justification shall take account of compliance with the UJICS Concept, the impact on security, scalability, cost of ownership, maintenance complexity, availability of skilled personnel and risks related to further operation and development of the System by the System Administrator.

The versions of programming languages, frameworks, libraries and System services shall be agreed with the System Owner.

The System shall operate on open-source UNIX-like operating systems. The operating system used shall belong to versions designated by their developer as Long-Term Support, LTS and shall provide long-term support, security updates and operational stability.

The distributed version-control system Git shall be used to store System code.

Where open-source solutions have equivalent functionality, preference shall be given to solutions that correspond to the proposed technology stack set out in Section 7.1.

7.1 Programming Languages, Frameworks and Libraries

The programming stack shall comprise:

1. front-end programming stack — Vue.js, version 3 or later;
2. back-end programming stack, with the choice justified by the Contractor:
    2.1. Python for work with data and analytics-related processes;
    2.2. Java for core UJICS-related processes.

The Contractor may propose alternative technical solutions. Where such solutions are proposed, the Contractor shall provide a justification for their selection and obtain approval from the System Owner.

7.2 Databases

The database shall be deployed in cluster mode and shall include mechanisms to prevent split-brain failures.

The following database types shall be used:

1. relational SQL database — PostgreSQL;
2. non-relational NoSQL database — MongoDB;
3. open-source REST-compatible object storage

Other types of databases may be used to meet specific System functional or non-functional requirements, provided that their use is justified, compatible with the target architecture and approved by the System Owner.

The Contractor may propose alternative technical solutions. Where such solutions are proposed, the Contractor shall provide a justification for their selection and obtain approval from the System Owner.

7.3 Integration Tools and APIs

System components shall interact with each other through standardised APIs and/or event-driven mechanisms.

The basic mechanism for synchronous interaction between System components shall be RESTful web services over HTTP(S), with data transmitted primarily in JSON format. Services shall support standard HTTP methods, namely GET, POST, PUT, PATCH and DELETE, in accordance with the implemented scenario. For scenarios requiring higher performance, bulk data processing, streaming transmission or low latency, the use of other protocols, data formats and asynchronous interaction mechanisms shall be permitted, provided that they are architecturally justified.

For integration with existing System components, the capability to operate using the SOAP protocol, with XML, and other data formats shall be provided. The System shall support the transformation of data between different formats.

The System shall enable automated electronic information interaction and data exchange between its components, both internally within the System and externally.

7.4 Core Infrastructure

7.4.1 Encryption Key and System Password Management

7.4.1.1 General Description

Encryption key and system password management shall constitute a centralised secure repository for System secrets, including passwords, certificates and API keys. The module shall provide the full lifecycle management of secrets, from generation and storage to rotation and revocation. It shall minimise the risk of disclosure of confidential infrastructure data and support scaling and geographical distribution mechanisms.

7.4.1.2 Main Functional Requirements

1. The module shall provide data storage with encryption appropriate to the relevant data-processing operation, including transmission, storage and other processing operations.
2. The module shall enable automatic rotation of passwords and keys on a schedule or in response to an event.
3. The module shall enable the issuance and automatic renewal of internal SSL/TLS certificates in order to ensure secure connections between subsystems through mutual TLS, mTLS.
4. The module shall provide an API for encrypting and decrypting data without transferring the encryption key itself to System components.
5. The module shall support mechanisms for splitting the repository access key among several administrators, for example through Shamir’s Secret Sharing scheme, so that no individual has complete control over the System.
6. Access to the secrets repository shall be strictly restricted in accordance with the principle of least privilege.

7.4.1.3 Integration and Use Requirements

1. The module shall support native authentication for services deployed in Kubernetes, K8s. Other System components shall not know the password of the secrets repository. They shall use their Service Account to obtain access.
2. The Contractor shall provide a mechanism for injecting secrets into functional System components through environment variables or temporary files directly into containers, so that developers of other System components do not need to develop complex integration code.
3. The module shall enable flexible access-rights configuration. For example, ‘Service A’ may read only the password for its own database and shall not be able to view the secrets of ‘Service B’.

4. Every attempt to access any secret shall be recorded, including who accessed it, when and which key or secret was requested.

7.4.2 Data Caching and In-Memory Storage of User Sessions

7.4.2.1 General Description

Data caching and in-memory storage of user sessions is a critical infrastructure component of the System. It shall be implemented as a distributed in-memory data store. The module shall serve as a high-performance intermediary between System components and primary databases. It shall support cluster-mode operation and geographical distribution in order to ensure fault tolerance and preservation of cached data in the event of failure of individual nodes.

The module shall address the following three strategic objectives:

1. externalisation of user session state from System components in order to enable their horizontal scaling;
2. preservation of drafts and user work context in conditions of unstable electricity supply and communications, with a limited time-to-live (TTL), to be determined at the Technical Specification stage;
3. acceleration of System component performance through caching of frequent queries and reduction of load on relational databases.

7.4.2.2 Main Functional Requirements

1. Provide a background auto-save mechanism for intermediate results of user activity.
2. Store the user work context, enabling a process to be resumed from the same point following an unexpected loss of connection or re-authorisation.
3. The module shall support caching of reference data by storing the results of resource-intensive database queries involving data that are frequently read but infrequently changed.
4. Support mechanisms preventing concurrent editing of the same object, for example a court case or document, by several users at the same time, unless collaborative editing of that object is permitted.
5. Manage the lifecycle of temporary data through Time-to-Live, TTL. It shall automatically remove obsolete sessions, drafts and outdated cache entries on the basis of configured retention periods.
6. Support shared sessions, ensuring that all instances of the same service have identical access to session and cache data.

7.4.2.3 Integration and Use Requirements

1. Stateless integration: System components shall not store any user or session state in their own operational memory. All session and user-state data shall be stored in this module through a standardised API.
2. Caching strategies: the module shall support different cache invalidation strategies, including time-based invalidation and invalidation triggered by changes to data in the primary database, in order to ensure that users receive up-to-date information.
3. The module shall be compatible with in-memory data-store protocols in order to ensure minimal latency in access to data.
4. The module shall be integrated with the authentication service in order automatically to invalidate temporary data and session keys when a session is terminated.

7.4.3 ‘File Content and Media Repository Management (S3)’ Component

7.4.3.1 General Description

File content and media repository management, S3, is a component for managing centralised object storage intended for the reliable, scalable and secure storage of object content, including PDF documents, audio and video recordings of hearings, photographic evidence and other materials.

Unlike traditional file systems, the component shall use an object-access model based on the S3 API, enabling the storage of petabytes of data and providing high-speed access.

7.4.3.2 Main Functional Requirements

1. S3 compatibility: the component shall support the Amazon S3 API protocol as an industry standard in order to ensure a vendor-agnostic approach and enable the use of MinIO, Ceph or cloud solutions.
2. The component shall ensure automatic or configurable retention of previous versions of an object when it is updated. Deletion of an object shall not result in the physical destruction of data without a specific Administrator command or dedicated configuration settings.
3. The component shall enable user-defined tags to be assigned to each file, for example case_id, document_type and security_level, allowing files to be searched and classified without querying the primary database.
4. The component shall enable configurable transfer of older files to cold storage, namely an archive, or their deletion after expiry of the retention period in accordance with rules established in the Electronic Archive service or configured separately, provided that the relevant item is not an electronic document or case file.
5. The component shall support multipart upload of large files, including hearing videos of 5–10 GB, with the ability to resume uploading after a connection failure.

7.4.3.3 Developer Tools and Integration Standards

The Contractor shall ensure that other development teams can integrate with the repository within the minimum possible timeframe. In particular, the Contractor shall:

1. provide a library or service for generating temporary links that enable the front end to upload files directly to S3, bypassing back-end services and thereby significantly reducing System load during mass document uploads;
2. provide ready-made configurations and wrappers, including SDKs, for standard S3 clients in Java, .NET and Python, already configured for operation within the System’s internal network;
3. provide tools and documentation enabling implementation of notification mechanisms and/or integration with existing System components;
4. develop and document a single path-naming policy, for example court-id/year/case-number/file-uuid, to prevent developers of different subsystems from creating inconsistent storage structures;
5. provide an abstraction layer for access to object storage that enables the provider or type of S3-compatible storage to be changed without changes to the business logic or application code of System components.

7.4.3.4 Security and Resilience Requirements

1. The module shall provide mandatory cryptographic protection of data in transit, using TLS, and at rest, using robust encryption algorithms of at least AES-256 strength.
2. Disabling or weakening cryptographic protection shall be permitted only for information that does not constitute restricted-access information and only where there is a separately documented decision of the System Owner adopted within the threat model and IPS.
3. The module shall support synchronous or asynchronous data replication between two or more geographically distributed data centres.
4. ICAP integration: every file uploaded to S3 shall automatically pass through a virus-scanning queue before becoming available to other users.

7.4.4 ‘Logging’ Component

7.4.4.1 General Description

The Logging component is a centralised repository intended to aggregate technical-event logs from all layers of System components, including infrastructure, databases, subsystems, Core Services and application software. The component shall serve as the primary data source for error investigation and technical diagnostics.

7.4.4.2 Main Functional Requirements

1. The component shall provide centralised real-time data collection from distributed infrastructure nodes and software components through lightweight agents.
2. The component shall store all events in a System-wide consistent format using standard fields, including Trace ID, Service Name and Severity Level.
3. The component shall support propagation of request context between System components in order to reconstruct the complete transaction path and support distributed tracing.
4. The component shall be configured and optimised for high-speed writing and search, with a retention period of 30 to 90 days depending on the criticality of the service.
5. The component shall provide:
   - 5.1. collection of service logs, system logs, security logs and technical integration logs;
   - 5.2. error logging that records:
     - 5.2.1. the unique transaction identifier;
     - 5.2.2. the error type;
     - 5.2.3. the stack trace;
     - 5.2.4. the severity level;
   - 5.3. logging of System configuration changes;
   - 5.4. logging of events relating to deployment of new services;
   - 5.5. time-stamp synchronisation through NTP;
   - 5.6. the ability to transmit logs to external Security Information and Event Management, SIEM, systems;
   - 5.7. compatibility with open-source log collection and analysis systems;
   - 5.8. configurable log-retention policies;
   - 5.9. recording of changes to logging settings;
   - 5.10. centralised aggregation of logs from all subsystems.
6. Protection requirements:
   - 6.1. the component shall provide:
     - 6.1.1. restriction of access to logs in accordance with roles;
     - 6.1.2. protection of logs against unauthorised modification;
     - 6.1.3. masking of sensitive data;
     - 6.1.4. log-integrity control.

7.4.4.3 Integration Requirements

1. The component shall use open standards for data collection and transmission.
2. The component shall automatically de-identify personal data, for example telephone numbers or Taxpayer Registration Numbers, in logs before their storage.

7.4.5 ‘Monitoring’ Component

7.4.5.1 General Description

The Monitoring component is an analytical layer that transforms raw data, including metrics and logs, into visual reports and operational alerts. The component shall be responsible for system health checks, monitoring and workload forecasting.

7.4.5.2 Main Functional Requirements

1. Visualisation: the component shall display key indicators in real time, including CPU, RAM, error rate, request latency, number of concurrent sessions and System component metrics.
2. The component shall provide a notification system independent of the core service, using SMS, Telegram, email or other channels, based on threshold values and anomalies, for example a sudden increase in HTTP 500 errors. The Contractor shall ensure that notifications can be sent in the event of:
   - 2.1. exceeding predefined threshold values;
   - 2.2. exceeding the defined response time of System components;
   - 2.3. approaching a limit value of System component operating parameters;
   - 2.4. reaching the maximum communication-channel capacity;
   - 2.5. detection of critical errors blocking operation;

2.6. failure of a UJICS component.
3. The component shall regularly verify the availability of public endpoints and internal services.
4. The component shall enable comparison of the current workload with historical data, for example workload during mass submission of reports.
5. The component shall enable the addition and management of business metrics and notifications required to identify potential issues.

7.4.5.3 Integration and Use Requirements

1. The component shall integrate with the Logging component for error-frequency analysis and directly with the containerisation platform for metric collection.
2. The Contractor shall enable developers of other System components to implement and connect a standard /health endpoint for polling by the Monitoring component. The Contractor shall develop and provide a specification for the JSON response of the /health endpoint, which shall be implemented by all other developers so that the Monitoring component can automatically identify the status of a service, including ‘Up’, ‘Down’ and other statuses.
3. Out-of-the-box metrics: the Contractor shall provide ready-made templates, including libraries and interceptors, for automatic collection of core metrics, including:
   3.1. response time, latency;
   3.2. number of errors, error rate;
   3.3. request throughput;
   3.4. other metrics to be determined at the Technical Specification stage.
4. The component shall enable developers of other System components independently to create and manage their own dashboards in the Monitoring system without involving the System Administrator.

7.4.6 ‘Message Queue’ Component

7.4.6.1 General Description

The Message Queue is an infrastructure service intended to provide asynchronous communication between UJICS subsystems and external information systems. The component shall act as an intermediary enabling an event-driven architecture and ensuring loose coupling of System components. The service shall be responsible for receiving, routing, temporary and/or persistent storage and guaranteed delivery of messages from publishers to subscribers.

7.4.6.2 Main Functional Requirements

The component shall provide:
1. support for the principal messaging patterns:
   1.1. Publish/Subscribe — for distribution of events to multiple services;
   1.2. Point-to-Point — for distribution of tasks among instances of the same service;
2. guaranteed delivery through retention of messages until successful acknowledgement of receipt by a subscriber, minimising the risk of data loss during restarts or updates of System components;
3. retry mechanisms through automatic retransmission of a message where the receiving service is temporarily unavailable, in accordance with a configured algorithm;
4. error handling through transfer of messages that could not be processed after a defined number of attempts to a dedicated dead-letter queue for further analysis and manual processing;
5. horizontal scaling through the dynamic increase of the number of consumers in order to ensure high throughput during peak workloads;
6. message prioritisation, enabling critical System events to be processed out of order or with higher priority.

7.4.6.3 Reliability and Performance Requirements

1. High availability: the component shall be deployed in cluster mode in order to eliminate a single point of failure.

2. Asynchronous interaction: resources of the sending service shall be released immediately after a message is accepted by the broker, without waiting for processing of the message by the recipient.
3. Isolation: each subsystem shall operate within its own logical namespace in order to prevent conflicts between queue names and unauthorised access to other parties' data.

7.4.6.4 Integration and Security Requirements

1. Protocol standardisation: the component shall support open interaction protocols, including AMQP 0.9.1, MQTT or Kafka Protocol.
2. Uniform data format: the component shall use a standardised message-body format with mandatory inclusion of metadata.
3. Monitoring integration: the component shall transmit metrics relating to queue length, message-processing speed and error counts to the Monitoring component.
   Security and audit:
   3.1. authentication of subsystems when connecting to the broker;
   3.2. encryption of traffic between sender, broker and recipient;
   3.3. access control: each service shall have access only to its designated queues and topics;
   3.4. logging of the publication and delivery of messages in the Logging component in order to support tracing of business processes.

7.4.7 'Audit Service' Component

7.4.7.1 General Description

The Audit Service is a centralised System component intended to record, preserve and display legally significant events and actions of users and administrators, as well as changes to data and the states of business objects.

The component shall establish an evidentiary record of actions performed within the System for the purposes of internal control, information security, official inspections, incident investigations and regulatory compliance.

7.4.7.2 Main Functional Requirements

The component shall provide:

1. Audit of user and administrator actions. The service shall record:
   1.1. login to the System;
   1.2. logout from the System;
   1.3. unsuccessful login attempts;
   1.4. creation and blocking of users;
   1.5. changes to roles and access rights;
   1.6. changes to security settings;
   1.7. actions requiring confirmation by QES;
   1.8. data export and import operations;
   1.9. search requests, in cases defined by the security policy.
2. Audit of operations involving business objects. The service shall record:
   2.1. creation, viewing, modification and deletion of objects, including documents, entities and records;
   2.2. changes to the status and state of documents;
   2.3. versioning of changes while retaining previous values;
   2.4. archiving, restoration, deletion or attempted access to archived materials;
   2.5. automatic or manual allocation of documents;
   2.6. information-interaction operations that have legal or security significance.
3. Audit-record content, including:
   3.1. date and time of the event, synchronised through NTP;
   3.2. unique event identifier;
   3.3. user identifier;

3.4. user role at the time the action was performed;
3.5. IP address and/or session identifier;
3.6. action type;
3.7. action object, including its type and identifier;
3.8. execution result, successful or unsuccessful;
3.9. additional context attributes, where necessary.

4. Immutability and retention of records:
4.1. audit records shall not be editable or deletable by users or administrators;
4.2. the integrity of records shall be controlled through hashing mechanisms or equivalent methods;
4.3. records shall be retained for the long term or indefinitely in accordance with the data-retention policy;
4.4. access to audit records shall be segregated in accordance with roles.

7.4.7.3 Requirements for the Provision and Use of Audit Data

The component shall enable audit data to be used by other UJICS services and subsystems. In particular, it shall:

1. provide access to a user's action history;
2. provide access to the change history of a specific object;
3. support filtering of records by:
3.1. period;
3.2. action type;
3.3. user;
3.4. object;
3.5. execution result;
4. support pagination and sorting of results;
5. enable audit information to be displayed in a user record or the Administrator console;
6. enable export of audit records in CSV format;
7. enable export in JSON/CEF format for integration purposes;
8. provide role-based access control for the API;
9. prevent the modification or deletion of records through the API.

7.4.7.4 Integration Requirements

The component shall provide:

1. integration with the Access Management, IAM, component to obtain user identification attributes;
2. integration with application subsystems through a standardised mechanism for transmitting audit events;
3. use of a standardised JSON data format for internal interaction;
4. the ability to transmit security events to external SIEM systems in standardised formats, including CEF or an equivalent format;
5. isolation of audit storage from direct access by application administrators;
6. time-stamp synchronisation through NTP in order to ensure correct event correlation;
7. the ability to scale in accordance with event volume.

8 REQUIREMENTS FOR SUPPORT AND MAINTENANCE OF THE INFORMATIZATION TOOL

Requirements shall be specified at the level of a user scenario for a System functionality group. Each scenario shall include the following sections: Objective, Preconditions, where applicable, Main and Alternative Scenarios or Functional Requirement Groups, where necessary, and Acceptance Criteria.

Requirements-modelling language shall be BPMN in accordance with DSTU ISO/IEC 19510:2017.

Project management systems, including ClickUp or equivalent systems through which the development process shall be managed, shall be provided by the System Administrator.

The System Administrator shall allocate NON-PROD infrastructure for development, including:

1. the GitLab source-code management system;
2. access to NON-PROD environments through a VPN.

Adaptation of the infrastructure to development requirements shall be carried out by the Contractor following agreement with the System Administrator.

8.1 Warranty Support Requirements

All System components shall be subject to warranty support for a period of 12 months, as established by the contract between the System Administrator and the Contractor. Warranty support shall include the correction of errors resulting from non-compliance of System components with the Technical Specification, the System Administrator's needs set out in these Technical Requirements or the UJICS Concept.

In order to ensure the proper operation of System components and compliance of their functions with the applicable requirements, the Contractor shall:

1. remedy all identified deficiencies in System components that do not comply with the requirements of the Technical Specification or the functional requirements within the timeframes defined in the Service Level Agreement, SLA, annexed to the contract;
2. update documentation where changes result in deviations from the state of System components at the time of delivery;
3. perform updates and/or restoration of System components, including updates to operating systems, network and communications equipment, server operating systems and system software, database management systems, application servers and web servers, in accordance with the requirements specified in the SLA annexed to the contract.

8.2 User Training Requirements

In order to ensure the effective use of System components, the Contractor shall prepare and provide training materials for users.

As a minimum, training materials shall include:

1. instructions on using the core functionality of services in the form of electronic help materials within the Wiki Service, describing typical user scenarios according to users' roles;
2. short video instructions for each module, where necessary, with a total duration not exceeding five hours.

Training materials shall be available electronically and shall be kept up to date to reflect changes in the functionality of System components.

The specific specialised format in which training materials concerning a particular aspect of System operation shall be presented shall be agreed during the development of the Technical Specification. The format of training materials shall be selected according to the complexity of the subject matter and the overall readiness of the relevant category of users to operate the System. In addition, training materials may take the form of a structured lecture course delivered through a specialised learning subsystem to be deployed by the System Administrator, video courses or automated tests with configurable questions and answer formats.

8.3 Documentation Requirements

The System shall be accompanied by the following documentation:

1. System User Manual for the available roles. The User Manual shall contain step-by-step descriptions of user actions for all operations, with visual illustrations, including interface screenshots.
2. System Administration Manual, including:
   - 2.1. instructions for initial System deployment, updating and rollback to a previous version;
   - 2.2. instructions for data backup and restoration;
   - 2.3. Helm charts and/or Ansible playbooks;
   - 2.4. SDLC policies and procedures, documented separately and implemented through GitLab CI/CD pipelines using GitLab Runner;
   - 2.5. monitoring and logging documentation describing monitored metrics, logs, audit events, notification rules, threshold values and incident-response procedures.
3. Developer and Tester Documentation, which shall:
   - 3.1. contain a list and description of supported methods;
   - 3.2. contain a list and description of request parameters;
   - 3.3. contain a list and description of response attributes;
   - 3.4. enable emulation of requests and responses, including a description of response status, such as success or error;
   - 3.5. enable the viewing of specifications and interactive use of API methods, including request execution and viewing of examples and schemas, through any OpenAPI-compatible tool, without being tied to a particular product;
   - 3.6. contain a description of the System data model and data structures, including the principal entities, their attributes, relationships, validation rules, reference directories, classifiers and data-exchange formats;
   - 3.7. contain a list of third-party components, libraries and services used, specifying their purpose, licences and use restrictions, as well as information confirming that their security was assessed during System development;
   - 3.8. contain a description of the release-management procedure, versioning, deployment of changes and maintenance of the change log, including release notes and changelog;
   - 3.9. include testing documentation, including a test plan, test scenarios with acceptance conditions, checklists, test data, test-result protocols, defect reports, test-coverage reports and test-execution reports.
4. System Architecture Description, indicating components, their interaction, deployment environments, external integrations, data flows and dependencies between services.
5. Testing Programme and Methodology for preliminary testing and/or pilot operation.
6. Test Protocol.
7. Test Certificate.
8. Training Programme and Training Materials for users holding different roles.

Documentation shall be complete, informative, clear, structured, easy to read, sufficient, unambiguous and internally consistent. Identical terms, definitions and identifiers shall be used throughout the documentation. Documentation shall be prepared in Ukrainian and provided electronically in a format that enables the text component to be edited.

9 REQUIREMENTS FOR ACCEPTANCE OF THE INFORMATIZATION TOOL

9.1. [QA] Requirements for Conducting Tests

Testing of System components shall be conducted to verify that the implemented functionality, integrations, security indicators and quality indicators comply with the Technical Specification and functional requirements and to confirm the readiness of System components for operation.

Testing shall cover all key functional capabilities of the services.

Testing shall be conducted in the designated NON-PROD environment in accordance with the 'Preliminary Test Programme and Methodology', which shall be developed by the Contractor and approved by the System Administrator before testing commences.

Test results shall be documented in test protocols and reports. These shall contain descriptions of the scenarios tested, test results, identified non-conformities, where applicable, and recommendations for remediation.

The Contractor shall remedy identified issues and defects within the timeframes agreed with the System Administrator, followed by re-testing.

9.1.1 Functional Testing

Functional testing shall be conducted at all stages of the development and enhancement of System components that involve the implementation or modification of functionality.

During testing, the correct implementation of System component functions shall be verified against the functional requirements of the Technical Specification.

The results of functional testing shall be documented in a Test Protocol signed by representatives of the System Administrator with the participation of the Contractor.

The Test Protocol shall be accompanied by a test report containing a description of the scenarios tested and identified observations, where applicable.

9.1.2 Integration Testing

Integration testing shall be conducted in respect of actually implemented interactions between System components, as well as interactions with external State information and communication systems and registers.

During testing, the correctness of data exchange and response processing, the resilience of integrations to errors, and the compliance of implemented mechanisms with the Technical Specification shall be verified.

9.1.3 Penetration Testing

Penetration testing and security testing shall be conducted to verify the level of protection of System components against unauthorised access, misuse of access rights, information leakage and other information security threats.

Security testing shall cover verification of user authentication and authorisation mechanisms, session management, segregation of access rights, protection of personal data and official-use data, as well as the resilience of System components to typical network and application attacks.

Following testing, a report shall be prepared containing a description of identified vulnerabilities, their severity, potential consequences and recommendations for remediation.

Where critical or high information security risks are identified, the Contractor shall ensure their remediation as soon as possible and provide confirmation that the System components are ready for re-testing. System components shall not be accepted by the System Administrator until all critical and high-severity findings have been remediated and the remediation has been verified through re-testing.

9.1.4 Load and Performance Testing

Load and performance testing shall be conducted to verify the System's ability to operate reliably under the forecast workload parameters defined in these Technical Requirements, determine its throughput and response times, and assess its resilience to peak loads.

Testing shall include verification of System operation under normal, target, peak and stress loads, analysis of server-infrastructure resource consumption, assessment of the performance of core usage scenarios and verification of recovery mechanisms following failures.

Following testing, a report shall be prepared containing a description of actual performance indicators, identified bottlenecks, an assessment of System compliance with non-functional requirements and recommendations for optimisation or scaling.

Where the System does not comply with established performance requirements, or critical errors are identified during load testing, the Contractor shall optimise the code and/or configuration and confirm that the System is ready for re-testing.

System components shall not be accepted by the System Administrator until the target performance and stability indicators have been achieved.

9.2 Requirements for Handover of Work Results

For the purposes of conducting preliminary testing of System components, a committee approved by the System Administrator shall be established.

The System shall successfully pass testing in accordance with the Preliminary Test Programme and Methodology developed by the Contractor on the basis of the Technical Specification.

The indicative period for performance of the work shall be from five to eight months from the date of signing the contract.

In addition, the Contractor shall include in its proposal a description of the approach to further enhancement and development of System functionality under the Change Request model. This description shall set out the procedure for initiating, assessing, approving, implementing and deploying changes, as well as the principles for estimating the cost and timeframe for implementing such changes.

All intellectual property rights, including exclusive rights, in the Software acquired by the System Owner apply only to the Software specifically created under the Agreement as part of the Project.

The full transfer of rights, including exclusive rights, to the Software entails the transfer of all intellectual property rights as established by Articles 424 and 440 of the Civil Code of Ukraine and Article 12 of the Law of Ukraine "On Copyright and Related Rights," without any restrictions on the methods of using the Software as specified by the Civil Code of Ukraine and the Law of Ukraine "On Copyright and Related Rights."

As a result of the transfer of property rights (including exclusive rights), the Contractor loses all property rights, and the System Owner acquires the right, including but not limited:

-to use the Software in all manners provided for by the Civil Code of Ukraine and the Law of Ukraine "On Copyright and Related Rights";

-to permit third parties to use the Software in the ways provided for by the Civil Code of Ukraine and the Law of Ukraine “On Copyright and Related Rights”;

-to prevent the unauthorized use of the Software, including prohibiting such use;

-to transfer (assign) the rights to the Software, in whole or in part, to third parties;

-to translate, adapt, modify (alter), update, or perform any other actions and/or changes to the Software or any part thereof;

-other intellectual property rights established by law.

The System Owner acquires intellectual property rights, including exclusive rights to the Software, for the duration of such rights in accordance with the laws of Ukraine. The intellectual property rights to the Software extend worldwide without restriction.

The transfer of intellectual property rights (including exclusive rights) to the Software by the Contractor to the System Owner shall be carried out on a no-cost basis. The cost of the intellectual property rights (including exclusive rights) to the Software is included in the cost of the Agreement for the creation of the Subsystem.

9.3 Requirements for Freedom to Operate

9.3.1. Requirements for Software Developed by the Contractor

By the time the System is transferred, the Contractor shall have duly regulated all legal relations with the authors and third parties engaged by it in the creation of the System and shall have acquired from them in full the proprietary intellectual property rights in the System. Such rights shall cover all methods of use of the work throughout the world and shall apply for the entire term of validity of proprietary intellectual property rights provided for by Ukrainian legislation. Detailed terms concerning proprietary intellectual property rights shall be set out in the relevant agreements concluded with the authors and third parties engaged in the creation of the System.