**ORDER**

**of the State Enterprise “Electronic Interoperability Center” under** **the State Committee for Information Technologies and Communications of the Kyrgyz Republic No. 2-a dated 1 March 2019**

**On Approving Technical Requirements for Operation of Members of the Electronic Interoperability System “Tunduk”**

In order to implement clauses 5, 6 and 10 of the Requirements for interaction of information systems in the electronic interoperability system “Tunduk” (hereinafter referred to as the EIS “Tunduk”) approved by Resolution No. 200 of the Government of the Kyrgyz Republic dated 11 April 2018, I hereby order:

1. To approve:

* Requirements for server hardware of organizations connecting to the EIS “Tunduk”;
* Requirements for registration in the Catalogue of interoperability solutions;
* Requirements for development and operation of adapters of information systems for making requests in the electronic interoperability system “Tunduk”.

2. The specialists of the State Enterprise “Electronic Interoperability Center” under the State Committee for Information Technologies and Communications of the Kyrgyz Republic shall take the necessary measures to fulfill the Requirements approved by this order.

3. A.Ch. Burzhuev, Deputy Director of the State Enterprise “Electronic Interoperability Center” under the State Committee for Information Technologies and Communications of the Kyrgyz Republic shall supervise the implementation of the order.

**Director  N.A. Kutnaeva**

Approved by Order No. 2-a of the State Enterprise “Electronic Interoperability Center” under the State Committee for Information Technologies and Communications of the Kyrgyz Republic dated 1 March 2019

**Requirements for Server Hardware of Organizations Connecting to the Electronic Interoperability System “Tunduk”**

**1. General Provisions**

1. These Requirements for server hardware of organizations connecting to the electronic interoperability system “Tunduk” (hereinafter referred to as the Requirements) have been developed in accordance with the Resolution No. 200 of the Government of the Kyrgyz Republic “On Approving the Requirements for Interaction of Information Systems in the Electronic Interoperability System “Tunduk” dated 11 April 2018.

2. These Requirements shall determine the technical requirements for server hardware, security server installation, communication channels, as well as for server room of organizations connecting to the electronic interoperability system “Tunduk”.

**2. Security Server Installation Requirements**

3. Security server shall be installed on the specialized server hardware of the organization. The server hardware must be located in a server room or in a room that meets security requirements.

4. Security server installation requires equipment with the following minimum specifications: 64-bit Intel dual-core, AMD, or another equivalent computing processor that supports AES hardware instructions, with 4096 MB of RAM and 3 GB of free hard disk space for a clean installation and additional disk space for storing transaction logs, with a USB 2.0 port, with two network interfaces or one in the case of an industrial-grade hardware network filter that supports DNAT.

**3. Communication Channel Requirements**

5. Communication channels shall be provided with a minimum of 1 Mbit or more to the external zone, which is necessary for installing updates of the operating system, 20 Mbit or more in the zone of the Kyrgyz Republic, as well as a public (global) IP address.

**4. Server Room Requirements**

6. The server hardware and software complex and data storage systems shall be located in the server room.

The server room shall be located in separate, impassable rooms without window openings. If there are window openings, they shall be closed or sealed with non-combustible materials.

Materials that do not emit and do not accumulate dust shall be used for the surface of walls, ceilings and floors. Materials with antistatic properties shall be used for flooring. The server room shall be protected from contaminants.

The walls, doors, ceiling, floor and partitions of the server room shall ensure the integrity of the room. The doors of the server room shall be at least 1.2 meters wide and 2.2 meters high, shall open outward or move apart. The design of the door frame shall not provide a threshold and a central pillar.

7. The server room shall be equipped with a raised floor and (or) a raised ceiling for placement of cable systems and utilities.

8. The passage of any transit communications through the server room shall be excluded. Regular and fire-fighting water supply, heating and sewerage routes shall be taken out of the server room and shall not be located above the server room on the upper floors.

9. Installation of communication channels for laying power and low-current cable networks of the building shall be carried out in separate or partitioned cable trays, ducts or pipes spaced from each other. Low-current and power cabinets shall be installed separately and locked.

Cables shall be laid through floors, walls and partitions in fireproof pipe sections which are sealed with non-combustible materials.

10. The server room shall be reliably protected from external electromagnetic radiation.

11. When placing the equipment in the server room:

- compliance with the rules of technical operation of consumers' electrical installations approved by the authorized body in the energy sector shall be ensured;

- fulfillment of requirements of suppliers and/or equipment manufacturer for installation (erection), load on floors and raised floor, taking into account the weight of equipment and communications shall be ensured;

- free service aisles shall be provided for equipment maintenance;

- control of microclimate system air flows shall be taken into account;

- organization of the system of raised floors and false ceilings shall be taken into account.

12. In case of technical maintenance of the equipment installed in the server room, the following shall be documented by a division or an authorized person:

- equipment maintenance;

- solving hardware and software problems;

- faults and failures, as well as the results of restoration work;

- post-warranty maintenance of critical equipment after the warranty period expires.

The form and method of documentation shall be determined independently by a state body or local government, organization.

13. Interference in the operation of the equipment in use shall be only possible with the permission of the authorized person.

14. The main and backup server rooms shall be located at a safe distance from each other in remote buildings. The requirements for backup server rooms are identical to those for main server rooms.

15. To ensure cybersecurity, fault tolerance and operational reliability:

1) equipment location methods shall be used in the server room to reduce the risks of threats, dangers and opportunities for unauthorized access;

2) a list of persons authorized to support the information infrastructure facilities installed in the server room shall be kept up to date;

3) the server room shall be equipped with systems of:

- access control and management;

- microclimate control;

- burglar alarm;

- video surveillance;

- fire alarm;

- firefighting;

- uninterruptible power supply;

- grounding;

4) Fault tolerance of the server room infrastructure should be at least 99.7 %.

16. The access control and management system shall provide authorized entry into the server room and authorized exit from it. The blocking devices and the design of the entrance door shall prevent access identifiers from being transferred in the opposite direction through the entrance door vestibule.

The central control unit of the access control and management system shall be installed in separate office premises, including the security post, which are protected from unauthorized access.

The access of the security personnel to the access control and management system software tools affecting the system operation modes should be excluded.

Power supply to the access control and management system shall be provided from the free group of the duty lighting panel. The access control and management system shall be provided with backup power supply.

17. The climate control system shall include air conditioning, ventilation and climate monitoring systems. The server room climate systems must not be combined with other climate systems installed in the building.

The temperature in the server room shall be in the range from 20 ºC to 25 ºC with a relative humidity of 45 to 55 percent.

The capacity of the air conditioning system should exceed the total heat output of all equipment and systems. The air conditioning system shall be provided with redundancy. Power supply to the server room air conditioners shall be provided by the guaranteed power supply system or uninterruptible power supply system.

The ventilation system shall ensure the supply of fresh air with filtration and heating of the incoming air in winter. Excessive pressure shall be created in the server room to prevent polluted air from entering the adjacent rooms. Protective valves controlled by a fire extinguishing system shall be installed on the air ducts of the supply and exhaust ventilation. The air conditioning and ventilation systems shall be automatically switched off by a fire alarm signal.

The climate monitoring system shall monitor climate parameters in server cabinets and telecommunication racks:

- air temperature;

- air humidity;

- air dustiness;

- air velocity;

- smoke content;

- opening (closing) of cabinet doors.

18. The security alarm system of the server room shall be separate from the building security systems. The warning signals shall be displayed in the 24-hour security room as a separate remote control. All entrances and exits of the server room as well as the internal volume of the server room are subject to control and protection. The security alarm system shall have its own redundant power source.

19. The location of the CCTV cameras shall be chosen to control all entrances and exits to the server room, space and passages near the equipment. The angle of view and resolution of the cameras should provide face recognition. The image from the cameras shall be displayed on a separate remote control in the 24-hour security room.

20. The fire alarm system of the server room shall be separate from the fire alarm system of the building. Two types of sensors shall be installed in the server room: temperature and smoke.

Sensors shall monitor the total server room space and the volumes generated by the raised floor and/or raised ceiling. Fire alarm system warning signals shall be displayed on a remote control in the 24-hour security room.

21. The fire extinguishing system of the server room shall be equipped with an automatic fire extinguishing unit independent of the fire extinguishing system of the building.

The fire extinguishing unit shall be placed directly in or near the server room in a specially equipped cabinet. The fire extinguishing system shall be started by early fire detection sensors that respond to smoke, as well as manual sensors located at the exit of the room. The fire extinguisher release delay time shall not exceed 30 seconds. The alarm from the fire protection system shall be sent out on the indoor and outdoor signal boards.

The fire extinguishing system shall issue commands to close the safety valves of the ventilation system and cut off the equipment power supply. The server room having a fire extinguishing system shall be equipped with exhaust ventilation.

22. The guaranteed power supply system shall provide two power inputs from different external power sources at ~400/230 V, 50 Hz and a stand-alone generator. All power sources shall be supplied to the reserve input machine, which automatically switches over to the reserve power input when the main input is shut down or the power supply is interrupted. Parameters of power supply lines and cross section of cores shall be determined on the basis of the planned total power consumption of equipment and subsystems of the server room. The power supply lines shall run in a five-wire circuit.

The guaranteed power supply system shall provide for power supply to the equipment and systems of the server room through uninterruptible power supply sources. The capacity and configuration of the uninterruptible power supplies shall be calculated taking into account all the equipment to be fed and the reserve for future development. The autonomy time from the uninterruptible power supplies shall be calculated taking into account the needs, as well as the necessary time to switch to backup lines and the time to start the generator in operating mode.

23. The grounding system of the server room shall be separate from the protective grounding of the building. All metal parts and structures of the server room shall be grounded with a common grounding bus. Each cubicle (rack) with equipment shall be grounded by a separate conductor connected to a common grounding bus. Open conductive parts of the data processing equipment must be connected to the main earthing terminal of the electrical installation. The earth conductors connecting the overvoltage protection devices to the main grounding bus must be the shortest and straightest (without corners).

24. It is prohibited to place the security server in offices, archives, auxiliary rooms and other premises.

25. All EIS “Tunduk” Members should limit physical and logical access to the security server to third parties who are not authorized employees of the organization. Granting access to the server equipment to unauthorized persons, if necessary, is possible only from the local network of the organization and under the supervision of an authorized person, with the event being recorded in the access granting registry.

26. The operator of the EIS “Tunduk” shall have the right to verify compliance of information systems of the EIS “Tunduk” Member with the legislation of the Kyrgyz Republic, technical requirements established by the operator of the EIS “Tunduk” if necessary.

27. The server equipment of the EIS “Tunduk” Member shall be placed only in the server room of the state body, local government and organization in accordance with the requirements to the server rooms established in these Requirements.

Approved by Order No. 2-a of the State Enterprise “Electronic Interoperability Center” under the State Committee for Information Technologies and Communications of the Kyrgyz Republic dated 1 March 2019

**Requirements for Registering Services in the Catalogue of Interoperability Solutions by Members of the Electronic Interoperability System “Tunduk”**

* + - 1. **General Provisions**

1. These Requirements for registering services in the Catalogue of interoperability solutions (hereinafter referred to as the Catalogue) by Members of the Electronic Interoperability System “Tunduk” (hereinafter referred to as the Requirements) have been developed in accordance with the Resolution No. 200 of the Government of the Kyrgyz Republic "On Approving the Requirements for Interaction of Information Systems in the Electronic Interoperability System “Tunduk” dated 11 April 2018.

2. These Requirements shall determine technical specifications for registration of information systems of ministries and agencies in the Catalogue, information entry, as well as data management.

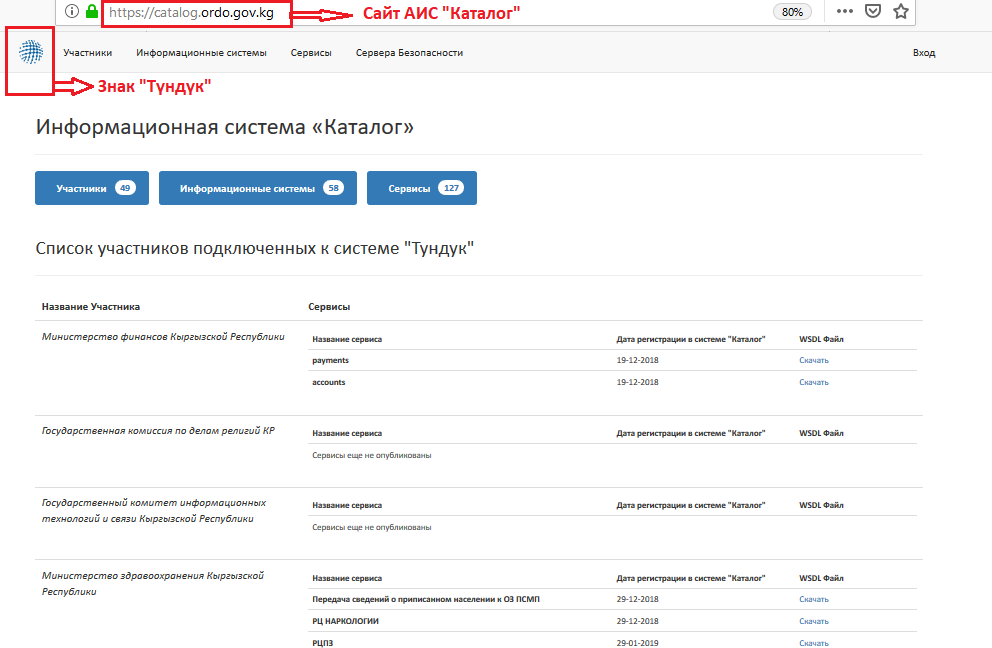
3. The Catalogue shall be maintained and filled out in the state and official languages.

4. The term used in these Requirements:

**User** – a responsible person appointed by the EIS “Tunduk” Member in the application for connection to the EIS “Tunduk” for editing information in the Catalogue about the EIS “Tunduk” Member.

**2. Using the Catalogue**

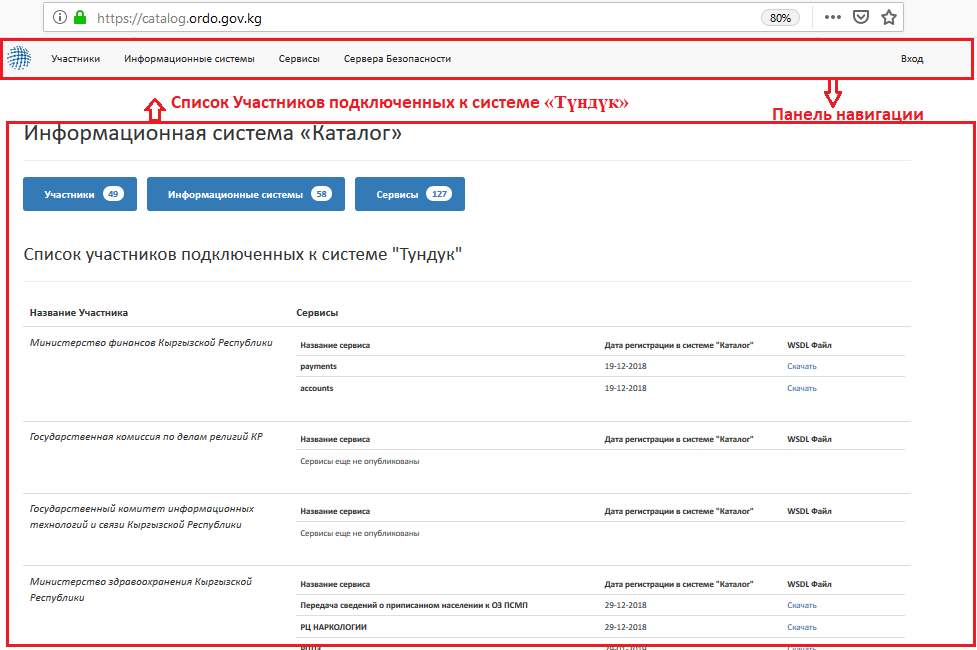
4. The main page of the Catalogue provides the User with an opportunity to view information on other EIS “Tunduk” Members connected to the Electronic Interoperation System “Tunduk” (hereinafter referred to as the EIS “Tunduk”). To go to the main page of the Catalogue one should follow the link <https://catalog.ordo.gov.kg/>. Also, to go to the main page of the Catalogue one should click on the sign "Tunduk" in the navigation bar.



5. The main page of the Catalogue consists of a navigation bar with the following information tabs:

* members – list of the EIS “Tunduk” Members;
* information systems – list of information systems of the EIS “Tunduk” Members (name, member, identifier);
* services – list of public and municipal services (name, information system, state body, identifier, version);
* security servers – list of servers installed for the EIS “Tunduk” Members.

Then follows “List of members connected to the “Tunduk” system”, where a list of organizations connected to the EIS “Tunduk” and their services is shown.

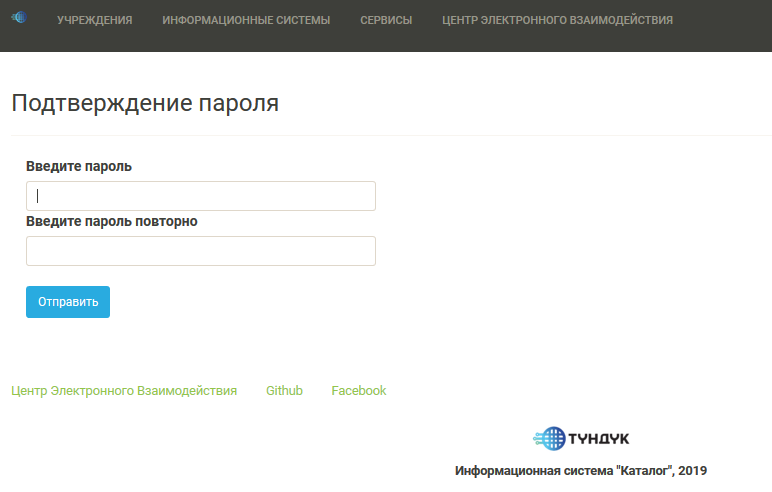


**3. User Registration in the Catalogue**

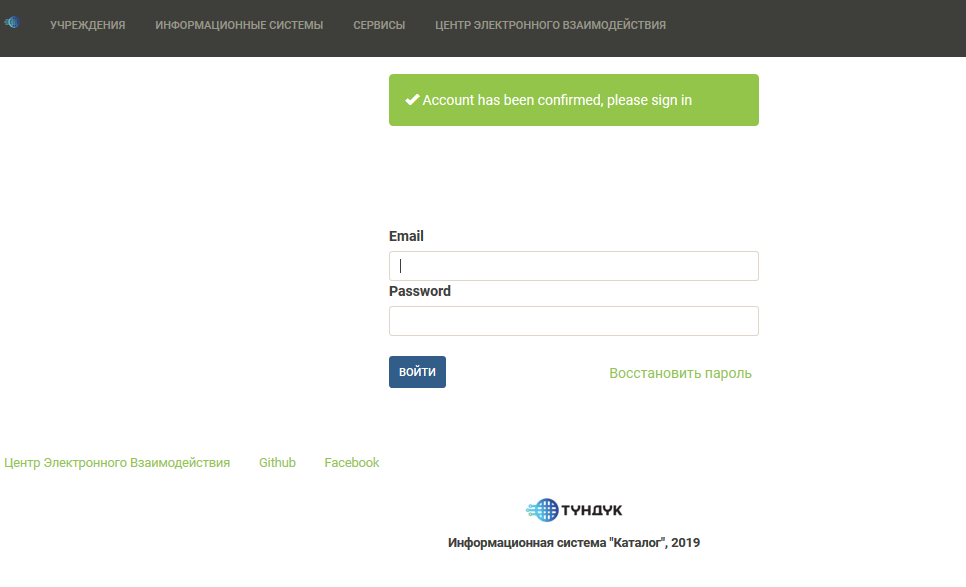
6. User registration in the Catalogue is carried out after positive consideration of the application for connection to the EIS “Tunduk”:

1) The Administrator of the State Enterprise "Electronic Interoperability Center" (hereinafter - SE "EIC") registers the User in the Catalogue, according to the completed application form for connection to the EIS “Tunduk”. After that, a link to enter the personal account in the Catalogue is sent to the User's e-mail address specified in the application for connection.

2) The User must follow a link to the password creation page in the Catalogue (the link is valid for 30 minutes from the moment of sending the invitation) and create an account password. The password must be at least 8 characters long and must not contain spaces.



1. After creating a password, the User logs in to his/her personal account, indicating his/her e-mail and the newly created password.



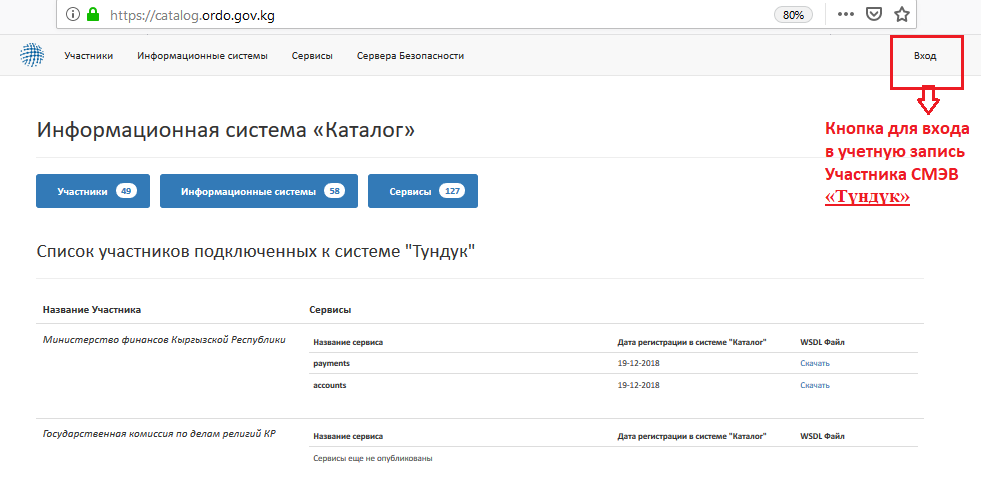
1. After logging in, the User will be redirected to the main page, which shows a list of members and services.

**4. Registration of Electronic Service in the Catalogue**

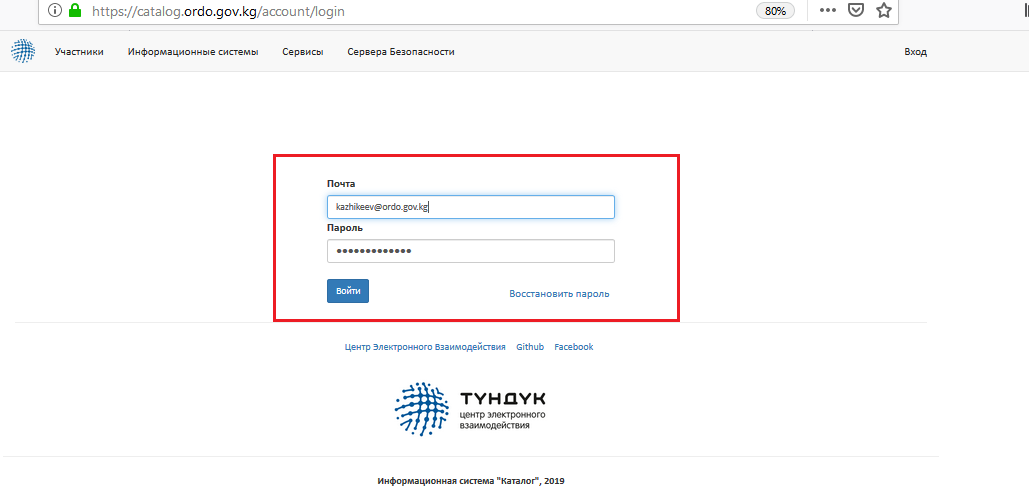
7. Names and descriptions should be in Cyrillic and have no abbreviations for comfortable use of the Catalogue, both for Administrator and Users.

8. In order to register an electronic service and make changes in the Catalogue, it is necessary to:

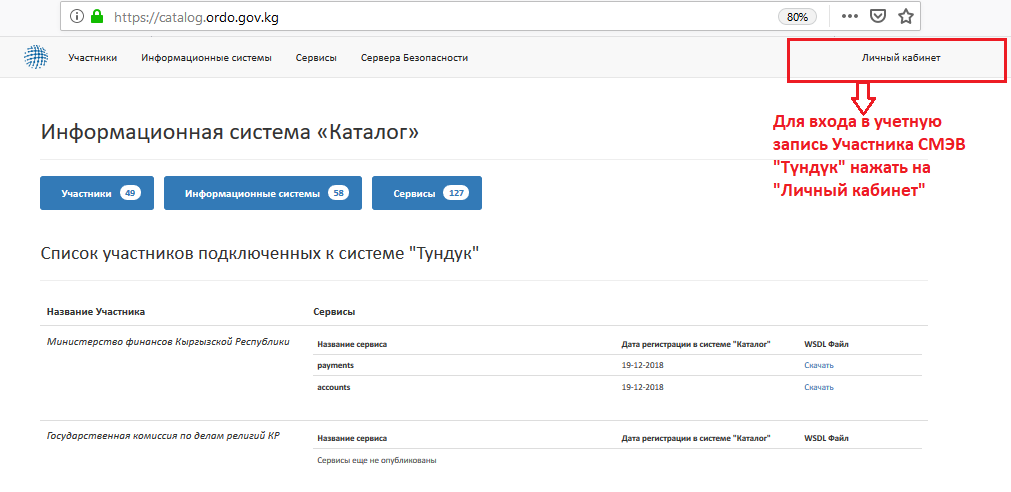
1. Enter a link *catalog.ordo.gov.kg* into the Internet browser.
2. Click on the "SIGN IN" button on the navigation bar of the Catalogue page.



1. Enter the e-mail (specified in the application) and the password created. Click on the "LOG IN" button.

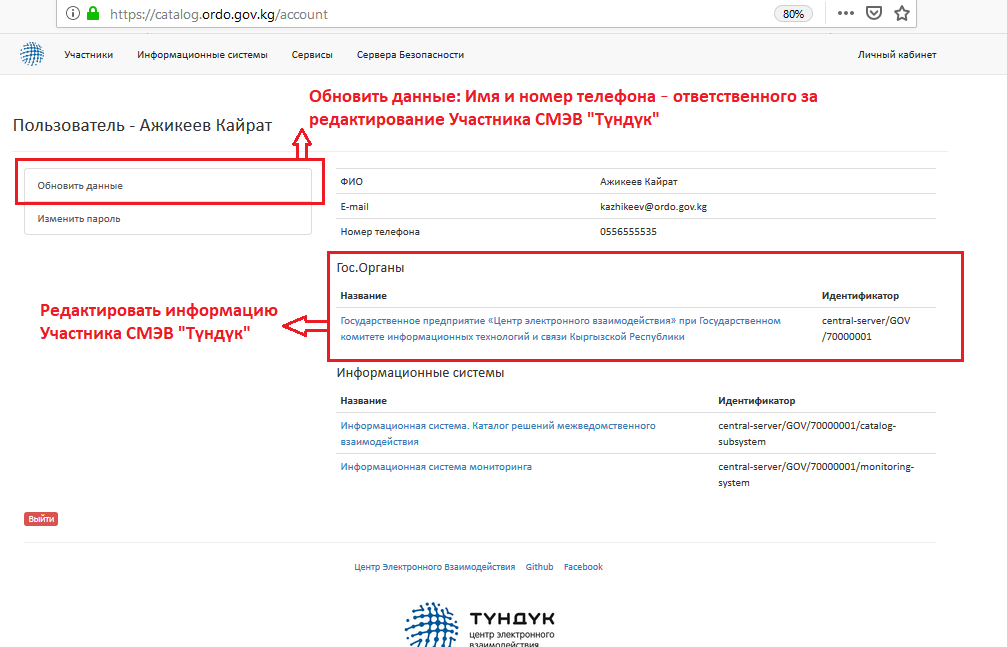


1. Click on the "Personal Account" button in the navigation bar.

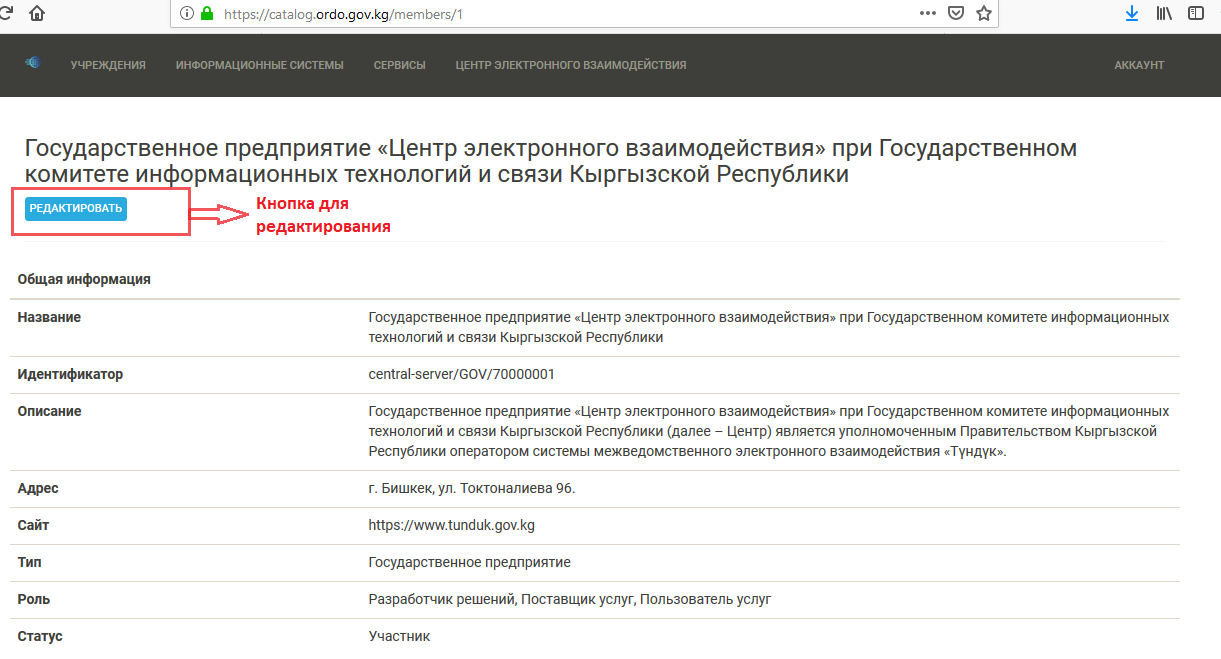


1. The window that appears will contain general information about the User and the EIS “Tunduk” Member (to which state, municipal body, their subordinate institutions or legal entities the registered information system belongs).

The User should click on the name of the organization in order to edit the information of the EIS “Tunduk” Member.

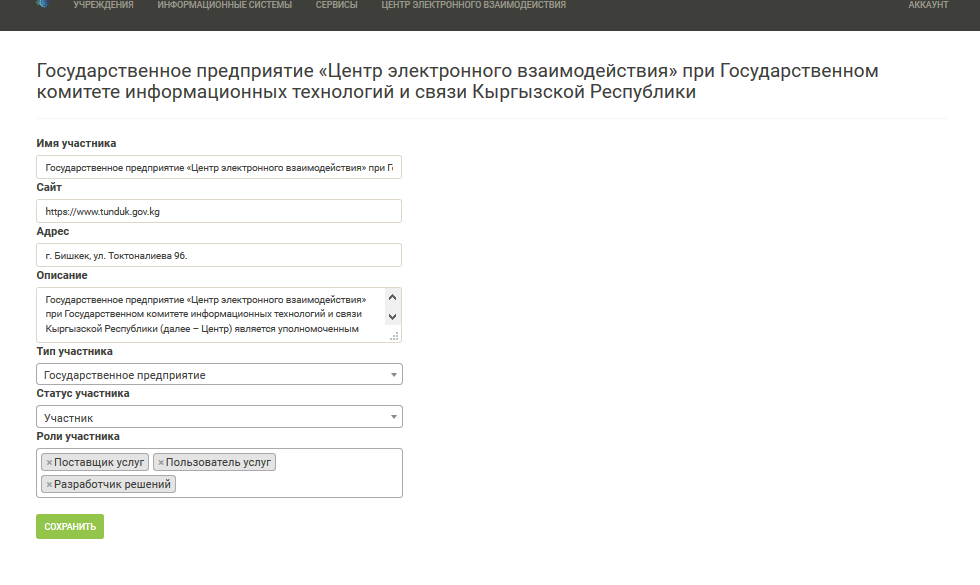


1. In order to enter the information of the EIS “Tunduk” Member it is necessary to click on the "EDIT" button.

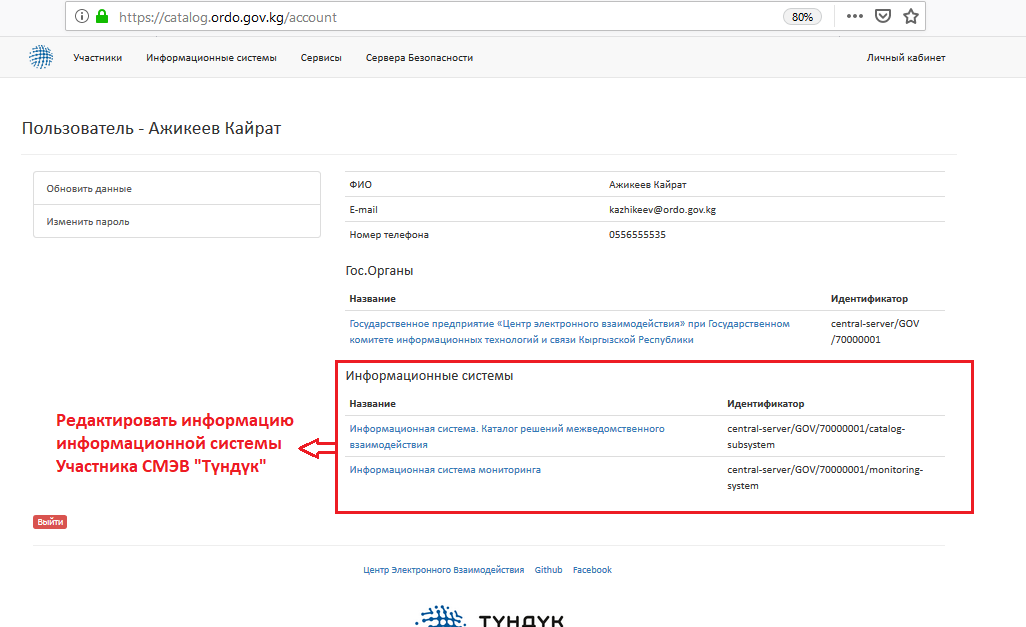


1. Next, it is necessary to fill in the fields with up-to-date information:

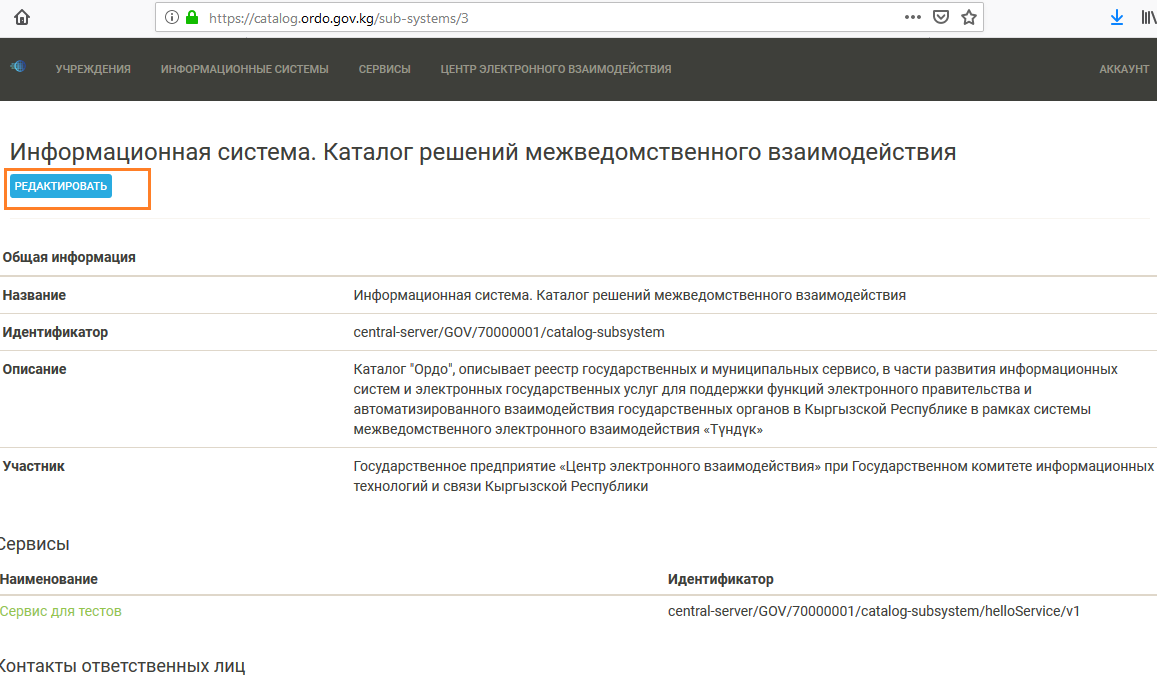
* member's name – official name of the EIS “Tunduk” Member;
* website – official website of the Member;
* address – actual location address;
* description – authority and scope of activities;
* member type – category of the Member (state bodies, local governments, state and municipal institutions and enterprises, legal entities and individuals);
* member status – it is necessary to choose one of the options indicating the current status of the EIS “Tunduk” Member in the Catalogue (member, removed);
* member roles – service provider, service user or solution developer.



1. Click on the “SAVE” button.
2. Click on the "Personal Account" button on the navigation bar.
3. Click on the name of the information system to edit the data of information systems of the EIS “Tunduk” Member.



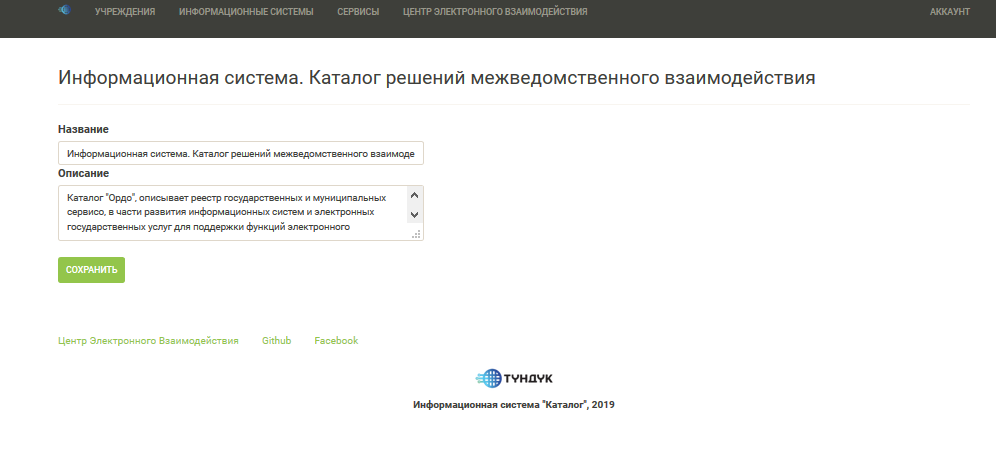
1. Click on the "EDIT" button to enter data about the information system of the EIS “Tunduk” Member.



1. Fill in the fields with up-to-date information:

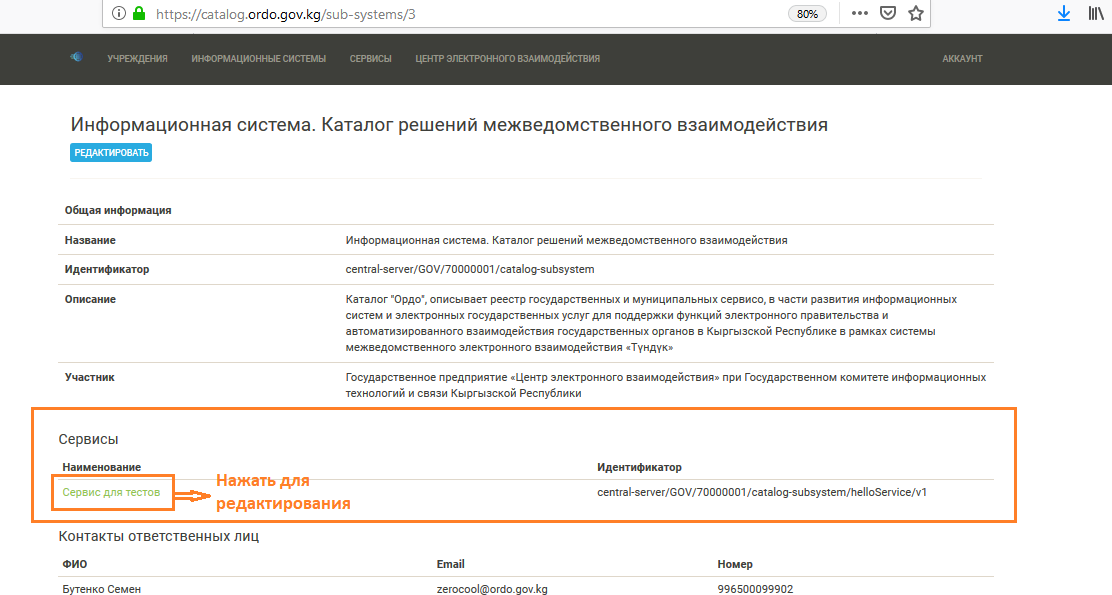
If this service is developed in accordance with the Plan for development of priority databases of state bodies, the name of the service must fully repeat the name specified in the Plan for development of priority databases:

* name – official name of the information system;
* description – tasks of the information system.



1. Click on the “SAVE” button.
2. The services are listed at the bottom of the “Information System” page.

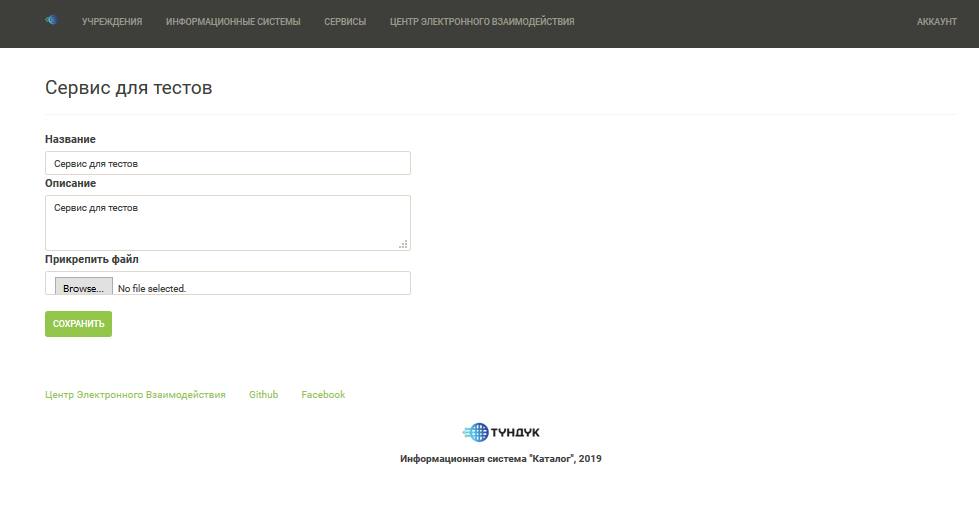
Click on the name of the service to edit information.



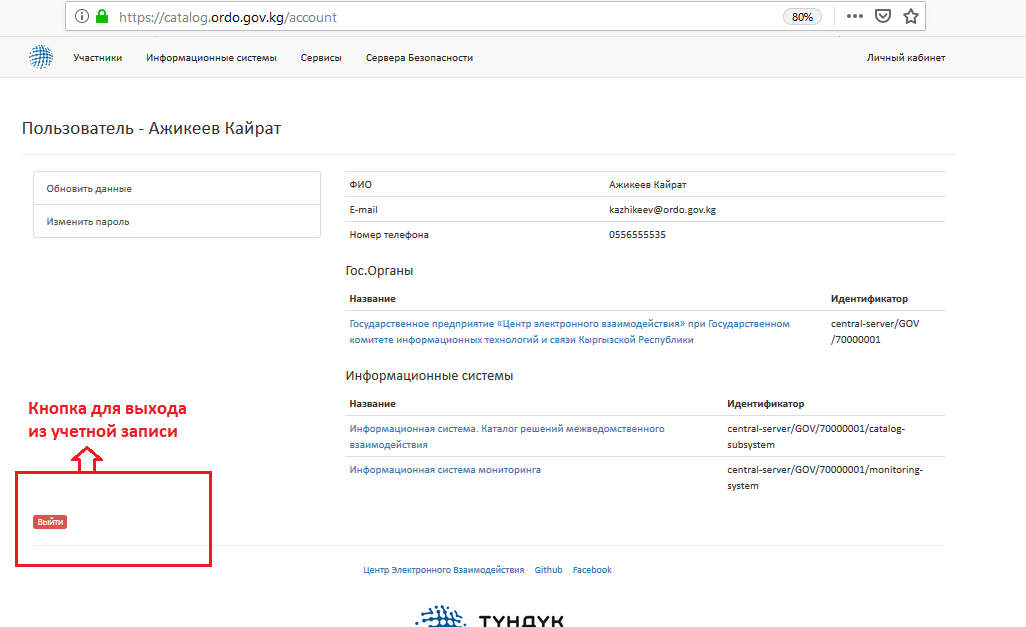
1. Click on the “EDIT” button.
2. Fill in the fields with up-to-date information:

* name – official name of the service;
* description – tasks of the service;
* attach the service documentation file – documentation required for connecting the EIS “Tunduk” Member’s service (at discretion).

1. After entering the information, click on the “SAVE” button.



9. In order to exit the User's personal account, click on the "Personal Account" button and click on the "EXIT" button at the bottom of the page.



Approved by Order No. 2-a of the State Enterprise “Electronic Interoperability Center” under the State Committee for Information Technologies and Communications of the Kyrgyz Republic dated 1 March 2019

# Requirements for Development and Operation of Information System Adapters for Making Requests in the Electronic Interoperability System “Tunduk”

# 1. General Provisions

1. These Requirements for development and operation of information system adapters for making requests in the Electronic Interoperability System “Tunduk” (hereinafter referred to as the EIS “Tunduk”) have been developed in accordance with the Resolution No. 200 of the Government of the Kyrgyz Republic "On Approving the Requirements for Interaction of Information Systems in the Electronic Interoperability System “Tunduk” dated 11 April 2018.

2. The following terms are used in these Requirements:

**Subsystem** – a part of the information system belonging to the Member of the Electronic Interoperability System “Tunduk” (hereinafter referred to as the EIS “Tunduk”).

**Central service** – a centrally defined short name for a particular service provided by the EIS “Tunduk” Member’s subsystem. The EIS “Tunduk” service is a web service based on SOAP (Simple Object Access Protocol), which is provided by the EIS “Tunduk” Member or subsystem and which can be used by other EIS “Tunduk” Members or subsystems.

3. These Requirements use the following terms to define the requirements for protocol implementation, in accordance with International Standard RFC 1123:

**Necessary, must** – is used to indicate that a specification requirement must be met;

**Recommended, should** – is used to indicate that a specification requirement should be met if valid reasons do not interfere;

**Perhaps, maybe** – is used to indicate that a specification requirement is optional and can be implemented as needed.

4. Implementation is considered incompatible if at least one of the **necessary** specification requirements of the protocol has been violated. Implementation that meets all **necessary** and **recommended** requirements is called fully compatible, and implementation that meets all **necessary** but not all **recommended** requirements is called conditionally compatible.

**2. Object Identification**

5. The EIS “Tunduk” uses unique identifiers. Identifiers consist of an object type and a sequence of hierarchical codes.

All identifiers begin with the code that identifies the EIS “Tunduk” instance. The code of the system uses the EIS “Tunduk” instance which is designated as "central-server" for the EIS “Tunduk” industrial instance.

6. The description of globally unique identifiers building for different types of entities is as follows:

When representing entities as strings, the format T:C1/C2/... is used, where T is the object type and C1, C2 are component codes.

*Note: this format is used only in this document. In messages and configuration files identifiers are presented in XML format.*

The EIS “Tunduk” Member – MEMBER: [INSTANCE]/ [member class]/ [member code], where the identifier consists of the following components:

- the code corresponding to the EIS “Tunduk” instance;

- the code defining the class of members (e.g. state body, private enterprise, individual. As a rule, member codes are issued by the body that guarantees the uniqueness of codes within a given member class);

- the member code which unambiguously identifies the belonging of the EIS “Tunduk” Member to the class.

***Example 1:***

*Member identifier: central-server/GOV/7432234/ is an organization registered in the EIS (central-server) with the state body class (GOV) and the code 7432234.*

*Subsystem - SUBSYSTEM: [subsystem owner] / [subsystem code]. The identifier for the subsystem consists of the EIS “Tunduk” member identifier, which owns the subsystem and its code. The subsystem code shall be selected by the EIS “Tunduk” member and it shall be unique within the subsystems of this member.*

***Example 2:***

*Subsystem identifier: central-server/GOV/7432234/highsecurity with a highhsecurity code belonging to the EIS “Tunduk” member from the previous example (MEMBER: central-server/GOV/7432234/).*

*Service - SERVICE: [service provider]/ [service code]/[version]. The service identifier consists of the service provider's identifier (either the EIS “Tunduk” member or the subsystem), the service code and its version. The service code is selected by the service provider. Version is an optional parameter and can be used to distinguish technically incompatible versions of the same service.*

***Example 3:***

*Service identifier: central-server/GOV/7432234/highsecurity/ getSecureData/v1 identifies the v1 version of the getSecureData service*

*central service - CENTRALSERVICE: /[central-server]/[service code]. The list of central services is managed by the operator of the EIS “Tunduk”, which also assigns unique service codes.*

***Example 4:***

*Central service identifier: central-server/populationRegisterpersonData identifies the central service that returns the person's data from the unified state register of population.*

**3. Message Format**

7. XML-based data formats for expressing identifiers are compiled as follows.

The data structures and elements defined in this section are located in the http://x-road.eu/xsd/identifiers namespace. The full XML schema is shown in the Annex.

***Example 5:*** *(schema definition header)*

*<? xml version="1.0" encoding="UTF-8"?>*

*<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"*

*elementFormDefault="qualified" targetNamespace="http://cyber.ee/xsd/identifiers"*

*xmlns="http://x-road.eu/xsd/identifiers">*

The complex type XRoadIdentifierType serves as a base for all other types of identifiers (derived from a restriction), which contains the union of all fields that may be present in different identifiers. The objectType attribute contains the type of identifier and can be used to distinguish between the EIS “Tunduk” Members and subsystems without resorting to conditions that verify the presence of separate fields.

***Example 6:***

*<xs:complexType name="XRoadIdentifierType">*

*<xs:sequence>*

*<xs:element minOccurs="0" ref="xRoadInstance"/>*

*<xs:element minOccurs="0" ref="memberClass"/>*

*<xs:element minOccurs="0" ref="memberCode"/>*

*<xs:element minOccurs="0" ref="subsystemCode"/>*

*<xs:element minOccurs="0" ref="serviceCode"/>*

*<xs:element minOccurs="0" ref="serviceVersion"/>*

*</xs:sequence>*

*<xs:attribute ref="objectType" use="required"/>*

*</xs:complexType>*

The XRoadObjectType enumeration lists all values of the objectType attribute.

***Example 7:***

*<xs:simpleType name="XRoadObjectType">*

*<xs:restriction base="xs:string">*

*<xs:enumeration value="MEMBER"/>*

*<xs:enumeration value="SUBSYSTEM"/>*

*<xs:enumeration value="SERVICE"/>*

*<xs:enumeration value="CENTRALSERVICE"/>*

*</xs:restriction>*

*</xs:simpleType>*

Then it is required to determine the elements and attributes used in XRoadIdentifierType.

***Example 8:***

*<xs:element name="xRoadInstance" type="xs:string"/>*

*<xs:element name="memberClass" type="xs:string"/>*

*<xs:element name="memberCode" type="xs:string"/>*

*<xs:element name="subsystemCode" type="xs:string"/>*

*<xs:element name="serviceCode" type="xs:string"/>*

*<xs:element name="serviceVersion" type="xs:string"/>*

*<xs:attribute name="objectType" type="XRoadObjectType"/>*

8. Complex types are defined to represent specific types of identifiers as follows.

XRoadClientIdentifierType is used to represent the identifiers that can be used by clients of the service, namely the EIS “Tunduk” Members and subsystems.

***Example 9:***

*<xs:complexType name="XRoadClientIdentifierType">*

*<xs:complexContent>*

*<xs:restriction base="XRoadIdentifierType">*

*<xs:sequence>*

*<xs:element ref="xRoadInstance"/>*

*<xs:element ref="memberClass"/>*

*<xs:element ref="memberCode"/>*

*<xs:element minOccurs="0" ref="subsystemCode"/>*

*</xs:sequence>*

*</xs:restriction>*

*</xs:complexContent>*

*</xs:complexType>*

XRoadServiceIdentifierType can be used to represent service identifiers.

***Example 10:***

*<xs:complexType name="XRoadServiceIdentifierType">*

*<xs:complexContent>*

*<xs:restriction base="XRoadIdentifierType">*

*<xs:sequence>*

*<xs:element ref="xRoadInstance"/>*

*<xs:element ref="memberClass"/>*

*<xs:element ref="memberCode"/>*

*<xs:element minOccurs="0" ref="subsystemCode"/>*

*<xs:element ref="serviceCode"/>*

*<xs:element minOccurs="0" ref="serviceVersion"/>*

*</xs:sequence>*

*</xs:restriction>*

*</xs:complexContent>*

*</xs:complexType>*

XRoadCentralServiceIdentifierType can be used to represent instance identifiers.

***Example 11:***

*<xs:complexContent>*

*<xs:restriction base="XRoadIdentifierType">*

*<xs:sequence>*

*<xs:element ref="xRoadInstance"/>*

*<xs:element ref="serviceCode"/>*

*</xs:sequence>*

*</xs:restriction>*

*</xs:complexContent>*

*</xs:complexType>*

9. Message headers and the requirement to fill them out are as follows.

Additional SOAP headers used in the EIS “Tunduk” are described according to this section.

In case the service client sends a request to the security server, one of the field services or centralService must be present. If the centralService field is used, the security server identifies the central service and automatically fills in the service field with the identifier of the specific service that implements the central service. In a request sent to the service, both fields **may** be present (the service field is present).

**Table 1. Description of message header parameters**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Field** | **Type** | **Mandatory or Optional** | **Description** | **Filling Requirements** |
| client | XRoadClientIdentifierType | Mandatory | Identifies the Client —  entity that initiates  service call. | To be filled in according to the EIS “Tunduk” protocol |
| service | XRoadServiceIdentifierType | Optional | Identifies the service called by the request. | To be filled in according to the EIS “Tunduk” protocol |
| centralService | XRoadCentralService-IdentifierType | Optional | Identifies the central service called by the request. | To be filled in according to the EIS “Tunduk” protocol |
| id | string | Mandatory | Unique identifier for the message. | It is **necessary** to use the following method of ID generation - 30 bytes of random data in Base64 encoding. |
| userId | string | Mandatory | The user whose action initiated a request.  The user identifier must be a two-letter ISO country code (e.g, KG12345678901). | userId — The user whose action initiated the request. The user identifier **should** be generated as:  1. Two-letter ISO country code with addition of personal identification number of the user (for example, KG20102199900011).  2. Another unique user identifier (e.g. the user identifier used in the AIS), this method of transmitting identifiers is **recommended** to be used in cases where it is impossible to identify the user for certain reasons (requests from law enforcement agencies), but it is **necessary** that the AIS requesting the information can identify a specific user. The information identifying the user by identifier **must** be stored on an ongoing basis, even in the event of dismissal of employees or decommissioning of AIS.  3. Another unique process identifier (e.g. background synchronization between registries) that initiated the data query. |
| requestHash | string | Optional | For answers. This field contains the hash of the SOAP request message. | This field is automatically filled in. |
| requestHash/  @algorithmId | string | Mandatory | Identifies the hash algorithm that was used to calculate the value of the Hash field request.  Algorithms are designated as URIs listed in the XML-DSIG  specification [DSI13]. | This field is automatically filled in by the security server service provider. |
| issue | string | Optional | Identifies an application, basis or document, which served as a basis for accessing the service.  This field is used to connect the request (and response) service to work procedures. | 1. It is **possible** not to transmit this information  2. It is **recommended** to transfer on what basis the data was requested (e.g. autocompletion of the form, debt verification, employment, etc.) |
| authentication  Method | string | Mandatory | Authentication method | 1. authenticationMethod should be one of the following:  EID - with an identity card (ID-CARD, DIGI-ID);  MID - with a mobile identity card (MOBILE-ID);  CERT - with another certificate;  EXTERNAL - via an external service (BANK-LINK);  PASSWORD - with a user identifier and password;  SYSTEM - when the request was sent by a cron task or other automatic process.  2. It is **possible** not to transmit this field if the reason for querying is not a specific AIS user (for example, cron task or other internal algorithms). |
| profileVersion | string | Mandatory | Version of the EIS “Tunduk” protocol. | Version 6 of the protocol 4.0 for the EIS “Tunduk” |

When responding, the service **must** copy all header fields from the request to the response.

10. The content of the message must use a SOAP coding agreement with documents/literals. Under this agreement, the content of the request must be wrapped in an element named foo and the content of the response must be wrapped in an element named fooResponse, where foo is the service name. The service name used in the wrapper element must match the serviceCode element of the service header field.

**4. Description of Services**

11. Services are described using the WSDL web services description language.

12. The EIS “Tunduk” supports various versions of services. Different versions of the service represent minor technical changes in the service description.

***Example 12:*** *The new version must be created when restructuring the service description (renaming or refactoring types in the XML schema) or when changing types or field names. When changing the service semantics or the content of these messages, it is necessary to create a new service with a new code.*

13. In the context of service contracts, services are considered without version, which means that all versions of the same service are considered equivalent.

*Note: This also applies to access restrictions applied on security servers, i.e. access controls are access codes without a version. For this to work, all versions of the same service must implement the same contract.*

14. Description of services by means of WSDL is performed as follows.

Service descriptions should be written in WSDL [WSD01] with the following restrictions and extensions.

The WSDL binding style/use combination must be a document/literal (binding style="document"; use="literal").

Service input and output parameters are described using the XML schema [XSD04a, XSD04b].

*Note: To avoid confusion on the part of the client whether an empty answer is a silent error or simply does not contain output records, it is recommended that for any service calls the answer should contain at least a nonempty scalar parameter. This parameter may be a non-technical error message (technical error messages must be returned with SOAP failures).*

Table 2 lists the elements that can be added to the WSDL for the transmission of information related to the EIS. The prefix namespace identifier is linked to the namespace "http://x-road.eu/xsd/identifiers".

**Table 2. WSDL elements for EIS “Tunduk” services**

|  |  |
| --- | --- |
| **Field** | **Description** |
| /definitions/binding/operation/@name | Code of the service |
| /definitions/binding/operation/  id:version | Version of the service |
| /definitions/portType/operation/  documentation/xrd:title | Name of the service (human readable— To be provided to the user) |
| /definitions/portType/operation/  documentation/xrd:notes | Description of the service (human readable— To be provided to the user) |
| documentation/xrd:notes  Description of the service (for displaying  to users)  /definitions/portType/operation/  documentation/xrd:techNotes | Description of the service (for developers to the user) |

**5. Final Provisions**

15. The EIS “Tunduk” Members are obliged to comply with these Requirements when developing adapters and working with them.

Annex to the Requirements for Development and Operation of Information System Adapters for Making Requests in the Electronic Interoperability System “Tunduk”

**XML Schema for Identiﬁers**

<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" targetNamespace="http://xroad.net/xsd/identifiers" xmlns="http://xroad.net/xsd/identifiers">

<xs:complexType name="XRoadIdentifierType">

<xs:annotation>

<xs:documentation>Globally unique identifier in the XRoad system. Identifier consists of object type specifier and list of hierarchical codes (starting with code that identifiers the XRoad instance).</xs:documentation>

</xs:annotation>

<xs:sequence>

<xs:element minOccurs="0" ref="xRoadInstance"/>

<xs:element minOccurs="0" ref="memberClass"/>

<xs:element minOccurs="0" ref="memberCode"/>

<xs:element minOccurs="0" ref="subsystemCode"/>

<xs:element minOccurs="0" ref="serviceCode"/>

<xs:element minOccurs="0" ref="serviceVersion"/>

</xs:sequence>

<xs:attribute ref="objectType" use="required"/>

</xs:complexType>

<xs:simpleType name="XRoadObjectType">

<xs:annotation>

<xs:documentation>Enumeration for XRoad identifier types.</xs:documentation>

</xs:annotation>

<xs:restriction base="xs:string">

<xs:enumeration value="MEMBER"/>

<xs:enumeration value="SUBSYSTEM"/>

<xs:enumeration value="SERVICE"/>

<xs:enumeration value="CENTRALSERVICE"/>

</xs:restriction>

</xs:simpleType>

<xs:element name="xRoadInstance" type="xs:string">

<xs:annotation>

<xs:documentation>Identifies the XRoad instance. This field is applicable to all identifier types.</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="memberClass" type="xs:string">

<xs:annotation>

<xs:documentation>Type of the member (company, government institution, private person, etc.)</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="memberCode" type="xs:string">

<xs:annotation>

<xs:documentation>Code that uniquely identifies a member of given member type.</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="subsystemCode" type="xs:string">

<xs:annotation>

<xs:documentation>Code that uniquely identifies a subsystem of given XRoad member.</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="serviceCode" type="xs:string">

<xs:annotation>

<xs:documentation>Code that uniquely identifies a service offered by given XRoad member or subsystem.</xs:documentation>

</xs:annotation>

</xs:element>

<xs:element name="serviceVersion" type="xs:string">

<xs:annotation>

<xs:documentation>Version of the service.</xs:documentation>

</xs:annotation>

</xs:element>

<xs:attribute name="objectType" type="XRoadObjectType"/>

<xs:complexType name="XRoadClientIdentifierType">

<xs:complexContent>

<xs:restriction base="XRoadIdentifierType">

<xs:sequence>

<xs:element ref="xRoadInstance"/>

<xs:element ref="memberClass"/>

<xs:element ref="memberCode"/>

<xs:element minOccurs="0" ref="subsystemCode"/>

</xs:sequence>

</xs:restriction>

</xs:complexContent>

</xs:complexType>

<xs:complexType name="XRoadServiceIdentifierType">

<xs:complexContent>

<xs:restriction base="XRoadIdentifierType">

<xs:sequence>

<xs:element ref="xRoadInstance"/>

<xs:element ref="memberClass"/>

<xs:element ref="memberCode"/>

<xs:element minOccurs="0" ref="subsystemCode"/>

<xs:element ref="serviceCode"/>

<xs:element minOccurs="0" ref="serviceVersion"/>

</xs:sequence>

</xs:restriction>

</xs:complexContent>

</xs:complexType>

<xs:complexType name="XRoadCentralServiceIdentifierType">

<xs:complexContent>

<xs:restriction base="XRoadIdentifierType">

<xs:sequence>

<xs:element ref="xRoadInstance"/>

<xs:element ref="serviceCode"/>

</xs:sequence>

</xs:restriction>

</xs:complexContent>

</xs:complexType>

</xs:schema>