Annex

Approved by
Resolution No. 200
of the Government
of the Kyrgyz Republic
dated 11 April 2018

REQUIREMENTS
for Interaction of Information Systems in the Electronic Interoperability System “Tunduk”

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

1. General Provisions

1. These Requirements shall determine the procedure for interaction of information systems in the Electronic Interoperability System “Tunduk” (hereinafter referred to as the EIS “Tunduk”), connection to it, its use and administration, general principles of information exchange (electronic documents) between information systems of state bodies, local governments, state institutions and enterprises, as well as legal entities and individuals in the implementation of electronic governance, including the provision of electronic public and municipal services.

2. Requirements for details and the form (format) of representation in electronic form of information of state bodies, local governments, interfaces of information exchange (electronic documents) of the EIS “Tunduk” and information systems connected to it shall be determined by interaction members in agreements on joining/interaction and registered in the Catalogue of Interoperability Solutions.

3. These Requirements shall not apply to information systems containing state secrets, the operation of which is determined by the legislation on protection of state secrets.

4. State bodies, local governments, state and municipal institutions and organizations providing public and municipal services or participating in their provision, shall provide the possibility of exchanging information (electronic documents) with information systems of other bodies and organizations through the EIS “Tunduk”, as well as ensure the transfer to digital (electronic) format of administrative procedures for the provision of public/municipal services and implementation of public/municipal functions.

5. Terms and definitions used in these Requirements:

adapter of the EIS “Tunduk” member’s information system - software that provides conversion of information requests transmitted via the EIS “Tunduk” into the format required by the information system of the EIS “Tunduk” member and back for interaction during service provision;

authentication certificate of a security server - an electronic document containing a public key, information about the key holder, scope of the key, signed by the certification authority that has issued it, certifying the authenticity of a security server and used for authentication of security servers when establishing a connection between security servers of information systems, which allows to establish with reliability members of electronic interaction who have sent and received an electronic document. The type (form) of the authentication certificate of the security server shall be determined by the certification authority in coordination with the operator of the EIS “Tunduk”;

applicant - state body, local government, state institution and enterprise, as well as legal entity and individual, exercising the powers of the holder (owner) of the information system, applying to the operator of the EIS “Tunduk” to connect an information system to the EIS “Tunduk” in accordance with these Requirements;

information system - information system of the EIS “Tunduk” member connected to the EIS “Tunduk” and registered in the Catalogue of Interoperability Solutions;

EIS “Tunduk” user interface - a standard, not central component of the EIS “Tunduk” designed to access the services of the EIS “Tunduk” members which do not have their own information systems;

Catalogue of Interoperability Solutions (hereinafter - the Catalogue) - information system that accumulates, records and provides information about the EIS “Tunduk” members, information systems of members connected to the EIS “Tunduk” and services provided by means of the EIS “Tunduk”, as well as about common classifiers and directories used by the EIS “Tunduk”. The form of the Catalogue as well as the list of information to be registered in the Catalogue shall be determined by the operator;

cybersecurity - preservation of integrity properties (which may include authenticity and fault tolerance), availability and confidentiality of information in information infrastructure facilities through the use of a combination of means, strategies, security principles, security guarantees, approaches to risk management, insurance, training, practical experience and technologies;

local monitoring center - software that monitors the status of security servers managed by the EIS “Tunduk” member and collects statistics on the use of the EIS “Tunduk” member's information system;

operator of the EIS “Tunduk” - a legal entity that performs the functions and authorities specified in these Requirements for coordination of activities of the EIS “Tunduk” members in order to implement and maintain the functioning of the EIS “Tunduk”;

connection to the EIS “Tunduk” - registration of the security server of the EIS “Tunduk” member;

EIS “Tunduk” - information technology and organizational environment ensuring safe and evidence-based exchange of information (documents) in the implementation of electronic governance, including the provision of electronic public and municipal services, performance of public and municipal functions;

security server - special software used to interface information systems of the EIS “Tunduk” members, which performs the functions specified in these Requirements;

member of the **EIS “Tunduk”** - state body, local government, state institution and enterprise, as well as legal entity and individual exercising the powers of the holder (owner) of the information system connected to the EIS “Tunduk”. Member of the EIS “Tunduk” is a service provider in the event that such services are provided through the EIS “Tunduk” to other members or a user of such services provided through the EIS “Tunduk” by other members; number of members of the EIS “Tunduk” is not limited;

certification authority - a legal entity determined by the Government of the Kyrgyz Republic, engaged in the creation and issuance of authentication certificates of security servers and electronic signature verification key certificates for information systems of the EIS “Tunduk” members, based on the public key infrastructure using the RSA algorithm (with digital signatures, time stamps (time-stamp functions), online certificate status protocol (OCSP), for the safe and evidence-based exchange of information (electronic documents) in the implementation of electronic governance, provision of electronic public and municipal services, performance of public and municipal functions;

service – an opportunity, registered in the Catalogue, for a member to receive information (documents) from the member's information system via the EIS “Tunduk”;

The list of provided/received information (documents) within the framework of the service shall be determined by the Service Level Agreement (SLA) concluded between the EIS “Tunduk” members and shall be registered in the Catalogue (in the service description).

central monitoring center - software that monitors the status of security servers and collects usage statistics in the EIS “Tunduk”.

Other terms and definitions shall be used in the meanings specified in the laws of the Kyrgyz Republic "On Electronic Governance", "On Electronic Signature", "On Access to Information Held by State Bodies and Local Governments", "On Public and Municipal Services".

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

2. Rights and Obligations of Electronic Interaction Members

6. The Operator of the EIS “Tunduk” shall:

- register members in the Catalogue, monitor the Catalogue maintenance, generate unified classifiers and directories of the EIS “Tunduk”;

- organize and coordinate connection of information systems to the EIS “Tunduk”;

- coordinate information system compatibility at the organizational level by concluding agreements on joining/interaction and exchange of information (electronic documents) with members;

- coordinate information system compatibility at the technical and technological level by providing information on open standards, specifications and protocols of information (electronic documents) exchange, formation of requirements for the development and operation of information system adapters;

- provide organizational and methodological support to the EIS “Tunduk” members;

- place the central components of the EIS “Tunduk” on its resources; ensure their technical support and uninterrupted operation;

- advise the EIS “Tunduk” members on issues related to the EIS “Tunduk”, as well as provide appropriate training;

- constantly monitor the use of the EIS “Tunduk” and address security incidents with appropriate responses;

- keep statistics on the use of the EIS “Tunduk”;

- prepare and implement the EIS ‘Tunduk” infrastructure development projects;

- perform other functions and powers to coordinate the activities of the EIS “Tunduk” members in order to implement and maintain the operation of the EIS “Tunduk”.

7. The EIS “Tunduk” members shall:

- manage security servers of their information systems;

- receive in the certification authority a security server authentication certificate and an electronic signature verification key certificate for their information systems in accordance with the laws of the Kyrgyz Republic;

- register information systems, resources and services in the Catalogue;

- administer their own information systems, which will interact via the EIS “Tunduk” security servers;

- provide cybersecurity for their information systems;

- develop adapters for their information systems;

- connect their information systems to the EIS “Tunduk” in accordance with the procedures established by these Requirements and the joining/interaction agreement;

- maintain the continuous operation of their information systems, adapters and security servers;

- bear responsibility for setting up access in their own security servers to the data of their information systems;

- generate and send, receive and process information (electronic documents) within the framework of services provided through the EIS “Tunduk”;

- ensure the completeness and accuracy of the information contained in electronic documents;

- use information (electronic documents) obtained through the EIS “Tunduk” in accordance with the legislation of the Kyrgyz Republic;

- exercise other powers and functions within the framework of ensuring the operation of the EIS “Tunduk”.

3. Procedure for Connecting to the EIS “Tunduk” and Registering Information Systems in the Catalogue

8. To carry out interaction and exchange of information (electronic documents) through the EIS “Tunduk”, the applicant shall submit an application for connection to the EIS “Tunduk” and sign an agreement on joining/interaction according to the forms established by the operator of the EIS “Tunduk”.

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

8-1. In case of compliance of the applicant's information system with these Requirements and technical requirements established by the operator of the EIS “Tunduk”, as well as with the legislation of the Kyrgyz Republic in the field of electronic governance and cybersecurity, the operator of the EIS “Tunduk” and the applicant shall enter into a joining/interaction agreement.

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

8-2. If the applicant's information system does not comply with the requirements set forth in clause 8-1 of these Requirements, the operator of the EIS “Tunduk” shall refuse to connect to the EIS “Tunduk” and notify the applicant of the need to eliminate the reasons that have led to the refusal to connect.

The applicant, after elimination of the reasons that have led to the refusal to connect, shall resubmit an application for connection to the EIS “Tunduk”.

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

9. After concluding the agreement on joining/interaction, the operator of the EIS “Tunduk” shall register the security server of the EIS “Tunduk” member.

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

9-1. After registering the security server of the EIS “Tunduk” member, the operator of the EIS “Tunduk” shall empower a person authorized by the EIS “Tunduk” member to register, enter and change data about the EIS “Tunduk” member in the Catalogue.

The EIS “Tunduk” member shall be obliged to register its information systems and all services provided in the Catalogue according to the requirements established by the operator of the EIS “Tunduk”. In case of creation of new services, after registration of the information system in the Catalogue, the EIS “Tunduk” member shall be obliged to register new services in the Catalogue before providing these services.

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

10. In order to connect to the EIS “Tunduk”, a member shall:

- ensure when connecting to the EIS “Tunduk” safe and uninterrupted operation of its information system in accordance with the requirements established by the operator of the EIS “Tunduk” and these Requirements;

- install a security server, create an information system adapter, if necessary - a local monitoring center, as well as ensure the operability of its information system in the EIS “Tunduk” pursuant to these Requirements;

- ensure archiving of log files of service requests with the required frequency of archiving and, in accordance with the list of archived information, identify persons entitled to access the archived log files, as well as determine the conditions of such access;

- ensure that the necessary security measures are applied to its information system and information protection;

- register in the Catalogue the services provided in accordance with these Requirements, keep the information available in the Catalogue up to date;

- conclude a service level agreement (SLA) with another member of the EIS “Tunduk”, specifying a list of received/provided data, organize and provide access to services during the period of interaction agreed upon by the parties;

- immediately notify the operator of the EIS “Tunduk” about service interruptions, planned and preventive works in its information system, about any violations and failures in the work of the EIS “Tunduk”;

- identify authorized persons who have the right to submit service requests through the EIS “Tunduk”, ensure their unambiguous identification in their information system and transfer the identifier of such an authorized person in the service request.

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

11. The application shall contain the following information:

- name and address of a member applying to connect to the EIS “Tunduk”;

- name (full name, position) of a member’s authorized employee (employees) responsible for maintenance and administration of the information system, for reliability of the information entered into the information system, as well as for connection and exchange of information (electronic documents) via the EIS “Tunduk”, authorized to sign on behalf of the member an agreement on joining/interaction with the operator of the EIS “Tunduk”.

12. (Repealed in accordance with Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

13. Before registering the information system, the operator of the EIS “Tunduk” shall check the data on the EIS “Tunduk” member, its information system, services provided, technical compliance of the information system and compliance of the information in the information system and its sources with the technical requirements established by the operator of the EIS “Tunduk”, these Requirements and legislation of the Kyrgyz Republic, as well as assess technical readiness of the member's information system for interaction through the EIS “Tunduk” pursuant to clause 10 of these Requirements.

14. The operator of the EIS “Tunduk” shall make a decision to:

- register a member and connect it to the EIS “Tunduk”;

- refuse registration indicating the circumstances to be eliminated.

15. (Repealed in accordance with Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

16. (Repealed in accordance with Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

17. When connecting to the EIS “Tunduk”, the operator of the EIS “Tunduk” and a member shall enter into a joining/interaction agreement that sets out the rights, obligations and responsibilities of the parties.

18. In case of registration of the information system in the Catalogue and connection to the EIS “Tunduk”, a member of the EIS “Tunduk” shall:

- receive a security server authentication certificate, an electronic signature for its information system in the certification center and register its security server in the EIS “Tunduk”;

- provide a security server authentication certificate, an electronic signature verification certificate of the information system to the operator of the EIS “Tunduk”;

- install private keys of the security server authentication certificate, electronic signature verification certificate of the information system(s) on its security server.

19. The operator of the EIS “Tunduk” shall:

- verify the data specified in the security server authentication certificate, electronic signature verification key certificate of the member's information system;

- register the security server authentication certificate, electronic signature verification key certificate of the member's information system in the EIS “Tunduk”.

20. After performing the procedures specified in this chapter, the information system of the EIS “Tunduk” member shall be considered ready for interfacing with the EIS “Tunduk” and interagency interaction.

21. The information included in the Catalogue shall be publicly available, except for personal information which is subject to the requirements of the legislation of the Kyrgyz Republic on protection of personal data (personal information).

22. No fee shall be charged from state bodies, local governments, state and municipal institutions, enterprises and their subordinate and territorial subdivisions for using the software of the EIS “Tunduk” components and the user interface of the EIS “Tunduk”.

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

23. Members of the EIS “Tunduk” shall bear costs for interfacing, development, administration of its information system, as well as for authentication at their own expense.

24. The operator of the EIS “Tunduk” may provide paid services.

Rates for services provided by the operator of the EIS “Tunduk” through the EIS “Tunduk” shall be established by the authorized state body in the field of antimonopoly regulation in accordance with the procedure specified by the Government of the Kyrgyz Republic.

(As amended by Resolution No. 296 of the Government of the Kyrgyz Republic dated 17 June 2019)

4. Invalidation of Connection to the EIS “Tunduk”

25. The information system of the EIS “Tunduk” member shall be disconnected from the EIS “Tunduk” if a member and/or its authorized person(s) or its information system does not comply with these Requirements.

26. Connection of the EIS “Tunduk” member may be invalidated by the operator and a member may be disconnected from the EIS “Tunduk” if:

- a member of the EIS “Tunduk” has provided inaccurate or incomplete information upon connection;

- a member of the EIS “Tunduk” has violated the terms set out in these Requirements or in the joining/interaction agreement;

- a member of the EIS “Tunduk” unfairly uses the services provided through the EIS “Tunduk”.

5. Architecture of the EIS “Tunduk”

27. Architecture of the EIS “Tunduk” shall comprise of the following components:

- security servers of the EIS “Tunduk” members;

- local monitoring centers of the EIS “Tunduk” members;

- central components of the EIS “Tunduk”.

28. The security server shall perform the following functions:

- encrypt and decrypt the transmitted information;

- generate log files, create evidentiary value for messages with digital signatures, time stamps;

- verify the access rights of the EIS “Tunduk” member using the services, manage the security server authentication certificates and electronic signature verification key certificates for signing and authentication;

- block access to the service for the information system of an unauthorized member of the EIS “Tunduk”;

- transmit information (electronic document) of the associated information system to another member of the EIS “Tunduk” as part of the services provided via a cryptographically secure channel;

- maintain log files.

29. The information system/systems may have several security servers running in parallel.

30. The local monitoring center shall not have access to data passing through the security server of the EIS “Tunduk” member. The EIS “Tunduk” member is not required to use a local monitoring center.

31. The central components of the EIS “Tunduk” shall include:

- registration server of the operator of the EIS “Tunduk”;

- security server of the operator of the EIS “Tunduk”;

- monitoring center.

32. The registration server of the operator of the EIS “Tunduk” shall send to the security server of the EIS “Tunduk” member the address of the security server of the required member – a service provider and transmit information about security server authentication certificates of the EIS “Tunduk” members.

33. The operator of the EIS “Tunduk” shall perform the procedure for registering the security server authentication certificates and electronic signature verification key certificates of information systems of the EIS “Tunduk” members in the central server.

34. The monitoring center shall monitor the status of security servers and collect statistics on the use of the EIS “Tunduk”. The central monitoring center shall have no access to data passing through the EIS “Tunduk”.

35. A member of the EIS “Tunduk” shall have the right to use the standard user interface of the EIS “Tunduk”, which has mechanisms for authentication and authorization of users. Services of the EIS “Tunduk” can be used through such a user interface of the EIS “Tunduk”.

6. Technical and Data Protection Requirements

36. The EIS “Tunduk” shall be used in accordance with the technical requirements established by the operator of the EIS “Tunduk”, by means of a security server having a security server authentication certificate, where the exchange of information (electronic documents) is encrypted and signed by the electronic signature of the information system of the EIS “Tunduk” member, as well as shall be provided with a cryptographically connected log file in order to ensure its authenticity and integrity.

Log files shall be kept for at least three years. The EIS “Tunduk” member may determine a longer period of time for storing log files.

37. The EIS “Tunduk” member shall be responsible for the security of its information system.

7. Final Provisions

38. Information systems from which it is necessary to obtain information for the provision of public or municipal services and performance of public or municipal functions shall be connected to the EIS “Tunduk”.

Other information systems may be connected the EIS “Tunduk”, including on a paid basis.

39. The volume and structure of information (electronic documents) to which access is provided through the EIS “Tunduk” shall be determined in accordance with the needs of the EIS “Tunduk” member and shall be indicated in the Catalogue and the agreement on joining/interaction with the EIS “Tunduk” member – a service provider. The EIS “Tunduk” member shall have the right to request information necessary for the provision of public or municipal services and/or performance of public or municipal functions.

The volume and structure of information accessible via the EIS “Tunduk” for legal entities and individuals shall be determined by the agreement between the EIS “Tunduk” members involved in the provision of the service.