Order N145/04

Of the President of the National Bank of Georgia

October 24, 2022

Tbilisi

Regarding the Approval of the Regulation on Common and Secure Open Standards of Communication

On the basis of Article 15, Clause 1, Sub-Clause "G" of the Organic Law of Georgia "On the National Bank of Georgia" and Article 221, Clause 6, Sub-Clause "D" of the Law of Georgia "On Payment System and Payment Services", **I order:**

Article 1

The Regulation on Common and Secure Open Standards of Communication shall be approved with the accompanying edition.

Article 2

This order shall come into effect on November 1, 2022.

National Bank President **Koba Gvenetadze**

Regulation on Common and Secure Open Standards of Communication

Chapter I

General Provisions

Article 1. Purpose and Scope

1. The purpose of the Regulation on Common and Secure Open Standards of Communication (hereinafter - the Regulation) is to ensure efficient and secure communication in the implementation of services for accessing account information and initiating payment, to define

uniform and secure open standards of communication for all participating parties, to promote the development of innovative products, with enhanced protection of communication sessions, to ensure the protection of confidentiality and integrity of information, as well as the interoperability of various technological solutions.

2. This Regulation defines common and secure open standards of communication between the account servicing payment service provider (hereinafter - "account servicing provider"), payment initiation service provider, account information service provider, payer, receiver and other payment service providers.

Article 2. Definition of Terms

1. For the purposes of this Regulation, the terms used therein shall have the following meanings:
    a) Authorized Provider – payment initiation service provider, account information service provider and payment service provider that has applied to the National Bank of Georgia for registration;
    b) Qualified Electronic Stamp Certificate – electronic stamp certificate issued by a qualified trusted service provider authorized in accordance with the Law of Georgia "On Electronic Documents and Electronic Trust Services" and which meets the requirements of the same law.
    c) Other terms used in this rule have the meanings provided by the Law of Georgia "On Payment System and Payment Services" and the legislation of Georgia.

Chapter II

General Requirements for Communication

Article 3. Requirements for Identification

1. The payment service provider is obliged to provide secure identification during communication between the payer's device and the receiver's device (including the post-terminal) in order to carry out electronic payment operations.

2. The payment service provider is obliged to ensure effective reduction of the risks of redirection of communication to an unauthorized person in the mobile application and other user interface of the payment service, through which electronic payment services are provided.

Article 4. Traceability

1. The payment service provider is obliged to implement processes that, during the provision of payment services, ensure the traceability of all payment operations, as well as other interactions with the payment service user (hereinafter - the "user"), other payment service providers and other persons (including trade/service facilities), in such a way that information on related events/actions occurring at each stage of the electronic payment operation can be traceable.
2. For the purposes of the Clause 1 of this Article, any communication session of the payment service provider with the user, other payment service providers and other persons (including trade/service facilities) relies on all of the following information:
    - the unique identifier of the session;
    - a security mechanism for detailed logging (recording) of the operation, including the operation number, time designation and all relevant data related to the operation;
    - time designation, which must be based on the International Coordinated Time System and must be synchronized with the official time signal.

Chapter III

Specific Requirements for Common and Secure Open Standards of Communication

Article 5. General requirements for access interfaces

1. An account service provider offering a payment account that can be accessed online must implement at least one interface that meets the following requirements:
    a) The account information access provider and the payment initiation service provider must be able to identify themselves towards the account servicing provider;
    b) The provider of access to account information must be able to request and receive information about one or more payment accounts specified by the user and the payment operations carried out on it through protected communication;

c) The payment initiation service provider must have the ability to initiate a payment order from the payer's payment account through secure communication. The payment initiation service provider must also be able to obtain the complete information related to the initiation of the payment transaction and the execution of that payment transaction that is required to perform the Payment Initiation Service and is available to the account service provider.

2. For the purposes of user authentication, the interface provided for in the Clause 1 of this Article shall allow the account information service provider and the payment initiation service provider to rely on all authentication procedures that the account service provider implements for the user. The interface must meet at least the following requirements:
   a) The payment initiation service provider and the account information service provider must have the ability to require the account service provider to initiate authentication based on the user's consent;
   b) Communication sessions between the account service provider, the account information service provider, the payment initiation service provider and the relevant payment service user must be established and maintained throughout the authentication process;
   c) The integrity and confidentiality of personalized security features and authentication codes transmitted by or through the payment initiation service provider and the account information service provider must be ensured.
3. The account service provider is obliged to ensure the compliance of its interface with the communication standards established by the international or European standardization organization.
4. The account service provider shall ensure that technical specifications are documented for any interface established for the purposes of this Regulation, in which regular processes, protocols and the means required for payment initiation service providers and account information service providers for the functional interoperability of their software and applications with the account servicing provider's system shall be defined.
5. The account service provider, upon request, shall provide free access to the authorized provider of the documentation specified in Clause 4 of this Article. The account service provider is obliged to ensure that the summary overview of the documentation is publicly available on its website.

6. The account service provider, except in emergency situations, must ensure that any change in the technical specification of the interface is made available to the authorized provider in advance, as soon as possible and at least 3 months before the change is implemented. The account service provider must document the emergency situations that led to the change. The account service provider is also obliged, upon request, to submit the documentation provided for in this clause to the National Bank of Georgia.
7. The account service provider must provide a test environment that includes connectivity and functionality testing support for the authorized provider to test its software and applications used to offer payment services to customers. It is not allowed to share sensitive information (including sensitive payment data) in the test environment.
8. The account service provider must ensure that the interface it implements always meets the requirements set forth in this Regulation. If the interface implemented by the account service provider does not meet the requirements defined by this regulation, the National Bank of Georgia is authorized to act in accordance with the current legislation of Georgia, so that payment initiation services and account information access services are not terminated or delayed, given that the relevant payment service providers providing these services meet the conditions specified in Article 8, Clause 6 of this Regulation.
9. For the purposes of this regulation, the payment service provider is obliged to be guided by the "Georgian Open Banking Standard" developed by the Georgian Banking Association, which is published on the website of the Georgian Banking Association - www.association.ge and/or www.openfinance.ge.
10. The payment service provider has the right to submit an alternative interface standard to the National Bank of Georgia for consideration, which will be in compliance with the requirements of this Regulation. The payment service provider is obliged to justify the superiority of the standard offered by him compared to the standard provided for in Clause 9 of this Article. The National Bank of Georgia will review the submitted interface alternative standard and, within 3 months, will approve or refuse the payment service provider to use it.

Article 6. Access Interface Conditions

In order to fulfill the requirements stipulated in Article 5 of this Regulation, the account service provider must fulfill one of the following obligations:

a) Implement a specialized interface for access to account information and payment initiation services;

b) Allow the authorized payment service provider to use the interface through which the account service provider authenticates and communicates with its customer.

Article 7. Requirements for Specialized Interface

1. The account service provider, which has implemented a specialized interface in accordance with Articles 5 and 6 of this Regulation, is obliged to ensure that the availability and performance of this interface, including support, at all times is at the same level as the interface used by the user to directly access his payment account online.
2. An account service provider that has implemented a specialized interface should establish transparent key performance indicators and service target levels, which must not be inferior to the corresponding indicators of the interface used by its users for direct access to the payment account online, both in terms of accessibility and data provided in accordance with Article 11 of this Regulation.
3. The account service provider shall perform monitoring and stress testing of the specialized interface, indicators and target levels provided for in this Article. Monitoring must be conducted through the account service provider's own IT infrastructure, from the server/servers on which the interface application provided for in the Clause 1 of this Article is not located. The account service provider is obliged to provide the National Bank of Georgia with documentation/information related to monitoring based on its request.
4. The specialized interface implemented by the account service provider shall not interfere with the provision of payment initiation and account information access services, which may include, among others:

    a) preventing the use by authorized providers of personalized security features provided by the account service provider to its own users;

    b) account service provider authentication or redirection to other functionality;

c) requiring additional verification of consent given by the user to the payment initiation service provider or account information access provider.

5. For the purposes of Clauses 1 and 2 of this Article, the account service provider is obliged to monitor the availability and functionality of the specialized interface. The account service provider is obliged to publish quarterly statistics on the availability and functionality of the specialized interface and the interface used by its user on its website.
6. The account service provider is obliged to provide the National Bank of Georgia with the statistical information provided for in Clause 5 of this Article. The National Bank of Georgia is authorized to post this information on its official website.

Article 8. Emergency Measures for Specialized Interface

1. When designing a specialized interface, the account service provider shall consider emergency measures strategy and plan for those cases, if:
   a) the specialized interface does not function in accordance with the requirements of Article 7 of this Regulation;
   b) there is an unexpected unavailability of the specialized interface;
   c) the system is out of order.
2. For the purposes of the Clause 1 of this Article, unexpected unavailability or system failure may be considered the case when 5 consecutive requests for access to the information required for the implementation of the payment initiation service or the account information access service have not been answered within 30 seconds.
3. Emergency measures should include a communication plan, according to which the payment service provider using the specialized interface will receive information about the measures to be taken to restore the functionality of this interface, as well as about the immediately applicable alternative means that may be available to the payment service provider in the cases provided for in the Clause 1 of this Article.
4. The account service provider and the authorized provider are obliged to immediately provide information to the National Bank of Georgia about the cases provided for in the Clause 1 of this Article.

5. As part of the emergency measures mechanism, the authorized provider must be able to use the interface used to authenticate users and communicate with the account service provider until the availability and functionality of the specialized interface is restored to the appropriate level provided for in Article 7 of this Regulation.
6. For the purposes of Clause 5 of this Article, the account service provider is obliged to ensure that the authorized provider is identifiable and that the latter can rely on the procedures implemented by the account service provider to authenticate the user. If the authorized provider uses the interface provided for in Clause 5 of this Article, he is obliged to:
    a) take the necessary measures so that it does not access, store and/or process data that is not used to provide the services requested by the user;
    b) ensure permanent compliance with the Regulations of Article 22, Paragraph 3 and Article 22, Paragraph 2 of the Law of Georgia "On Payment System and Payment Services";
    c) record (log) the data accessed through the interface managed by the account service provider for its users. Based on the request of the National Bank of Georgia, the authorized provider is obliged to provide it with the mentioned records (logs) without unjustified delay.
    d) Based on the request of the National Bank of Georgia, without unjustified delay, provide it with comprehensive justification regarding the user's use of the interface intended for direct access to his payment account online;
    e) immediately inform the account service provider.
7. The National Bank of Georgia is authorized to release the account service provider who decides to use a specialized interface from the obligation to implement the emergency measures mechanism specified in Clause 5 of this Article, if this interface meets all the following conditions:
    a) the specialized interface meets all the requirements specified in Article 7 of this Regulation;
    b) the specialized interface has been designed and tested in accordance with Article 5, Clause 7 of this regulation and meets the requirements of the authorized provider;
    c) the specialized interface has been widely used by the payment service provider for at least 3 months for the implementation of account information access services and payment initiation services;
    d) any problems related to the specialized interface were resolved without undue delay.

8. The National Bank of Georgia is authorized to cancel the exception granted in accordance with Clause 7 of this Article, if the account service provider fails to ensure the fulfillment of the conditions stipulated in Sub-clauses "A" and "D" of the same Clause within 2 consecutive calendar weeks. In this case, the account service provider is obliged, in the shortest possible time, but no later than 2 months, to ensure the implementation of the mechanism of emergency measures specified in Clause 5 of this Article.
9. If an account service provider allows an authorized provider to use the interface through which it authenticates and communicates with its user, it is exempt from the requirements of this Article.

Article 9. Certificates

1. For the purposes of identification defined by Sub-clause "A" of the Clause 1 of Article 5 of this Regulation, the payment service provider is obliged to use a qualified electronic stamp certificate and/or a qualified website authentication certificate.
2. For the purposes of this Regulation, the identification code provided for in Article 2, Sub-clause "K" of the Law of Georgia "On Electronic Document and Electronic Trust Services" shall be for the account service provider, the payment initiation service provider and the account information access provider, as well as the registration/license number granted by the National Bank of Georgia, which is publicly available on the official website of the National Bank of Georgia.
3. For the purposes of this Regulation, the qualified electronic stamp certificate or the qualified website authentication certificate provided for in the Clause 1 of this Article must include the following additional information, in Georgian and/or English:
    a) Authority of the payment service provider, which may include one or more of the following:
        i. account services;
        ii. payment initiation services;
        iii. account information access service.
        iv. the regulatory body by which the payment service provider is registered/licensed.
4. The requirements specified in Clause 3 of this Article shall not affect the recognition and interoperability of a qualified electronic stamp certificate or a qualified website authentication certificate.

Article 10. Communication Session Security

1. In order to ensure the protection of confidentiality and integrity of data, the account service provider, account information access provider and payment initiation service provider, when exchanging data via the Internet, are obliged to ensure reliable encryption of data during each session of communication between the parties using widely recognized encryption technologies.
2. The account information access provider and the payment initiation service provider are obliged to ensure that the access session offered by the account service provider is as short as possible and that all such sessions are actively terminated upon completion of the requested action.
3. During parallel network sessions with the account service provider, the account information access provider and the payment initiation service provider are obliged to ensure that these sessions are securely connected to the corresponding sessions established with the user(s) so that any messages or information exchanged between the parties are not misdirected.
4. The account information access provider and the payment initiation service provider shall, when communicating with the account service provider, provide a unique reference to each of the following:
    a) the user or users and the corresponding communication sessions, so that multiple requests from the same user or users can be distinguished from each other;
    b) an initiated payment transaction uniquely identified by the payment initiation service;
5. The account service provider, account information service provider and payment initiation service provider shall ensure that personalized security features and authentication codes cannot be read directly or indirectly by any employee at any time during the exchange.
6. The account service provider, account information service provider and payment initiation service provider shall, in the event of doubt regarding the confidentiality of personalized security features within their area of responsibility, immediately notify the relevant user and the issuer of such personalized security features.

Article 11. Data Exchange

1. The account service provider is obliged to meet the following requirements:

a) provide the account information service provider with the same information on the payment account and the payment operations carried out on this account, which is available to the user in case of direct access to the account by him, except for sensitive payment data;

b) upon receipt of the payment order, immediately provide the payment initiation service provider with the same information about the initiation and execution of the payment operation that it provides to the user or provides access to it when the user initiates the payment operation directly with him.

2. In the event of an unforeseen circumstance and/or error during the data exchange, identification or authentication process, the account service provider is obliged to send a notification to the payment initiation service provider and the account information service provider indicating the reason for this delay.
3. If the account service provider offers the user a specialized interface in accordance with Article 7 of this Regulation, in the event of an unforeseen circumstance and/or error, through this interface, it shall be possible to send a notification of such a circumstance or error by a payment service provider that detects an unforeseen circumstance and/or error to another payment service provider participating in the same communication session.
4. The provider of access to account information is obliged to implement an appropriate and effective mechanism that ensures the restriction of access to the payment account and information to which the user has not given explicit consent.
5. The payment initiation service provider is obliged to provide the account service provider with the same information that the account service provider requests from the user when the latter initiates a payment operation directly with him.
6. The account information service provider must be able, in order to provide the account information access service, to receive information about the payment account specified by the user and/or the payment transaction carried out on that account, which is held by the account service provider in one of the following cases:

a) if the user actively requests this information;

b) if the user does not actively request information and the number of said requests does not exceed four in a 24-hour period, unless with the user's consent, the account information

access provider and the account service provider have agreed on a higher frequency of requests.

Chapter IV

Transitional Provisions

Article 12. Transitional Provisions

1. The account service provider is obliged to comply with this provision:
   a) ensure fulfillment of the requirements provided for in Clause 4 of Article 5 no later than December 1, 2022;
   b) ensure fulfillment of the requirements provided for in Article 5, Clause 7 no later than January 1, 2023;
   c) ensure compliance with the requirements of publication of quarterly statistics of the availability and functioning of the interface provided for by Clause 5 of Article 7 no later than October 1, 2023;
   d) ensure compliance with the requirements provided for in Clause 2 of Article 8 no later than October 1, 2023;
   e) ensure compliance with the requirements provided for in Clause 5 of Article 8 no later than October 1, 2024.
2. The account service provider, who wants to benefit from the exception provided for in Article 8, Clause 7 of this Regulation, is obliged to submit a relevant application to the National Bank of Georgia by January 1, 2024.
3. For the purposes of Sub-Clause "A" of the Clause 1 of Article 5 of this Regulation, until December 31, 2026, it is possible to use the certificate issued by the relevant organization provided for in the EU Regulation N910/2014, the information about which is placed in the lists created in accordance with Article 22 of the same Regulation.