Pursuant to Article 47 paragraph 1 item 6 of the Law on the National Bank of the Republic of North Macedonia (Official Gazette of the Republic of North Macedonia No. 158/10, 123/12, 43/14, 153/15, 6/16, 83/18 and Official Gazette of the Republic of North Macedonia No. 110/21), and Article 124 paragraph 7 and Article 125 paragraph 3 of the Law on Payment Operations (Official Gazette of the Republic of Macedonia No. 90/22), the National Bank of the Republic of North Macedonia Council has adopted the following

DECISION
on requirements for strong customer authentication and common, secure and open standards of communication

I. GENERAL PROVISIONS

1. This Decision shall closely prescribe the following:

   - requirements for strong authentication between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers for the purposes of identification, authentication, reporting and informing, protecting the confidentiality and the integrity of the payment service user's personalized security credentials, as well as exemptions from the standards for strong authentication and
   - standards for interfacing and secure communication to be applied when interfacing the account servicing payment service provider who provide direct online access to payment accounts, with account information service providers, payment initiation service providers and payment service providers using card-based payment instruments, as well as the terms under which the National Bank may facilitate the application of continuity standards.

2. The terms used in this decision shall denote the following:
   - **Qualified certificate for electronic seal** shall denote a certificate for electronic seal issued by a qualified confidential service provider eligible under the Law on Electronic Documents, Electronic Identification and Confidential Services, which refer to a qualified certificate for electronic seal.
   - **Authentication redirection** shall denote a method whereby the confirmation of identity of the user of payment services to account information service providers and payment initiation service providers automatically redirects to the infrastructure (website or application) of the account servicing payment service provider for the purpose of registering the user's security credentials.
   - **Authentication decoupling** shall denote a method whereby the confirmation of identity of the user of payment services to account information service providers and payment initiation service providers automatically redirects to another communication session connected to the infrastructure of the account servicing payment service provider for the purpose of registering the user's security credentials.

- **Authentication embedding** shall denote a method whereby the payment service user's security credentials are provided to account information service providers and payment initiation service providers to confirm the payment service user's identity without communicating with the account servicing payment service provider.
- **Secure environment** shall comprise at least the payment service provider's premises, the Internet environment provided by the payment service provider or other similar secure websites used by the payment service provider and its ATM services, which are not under the payment service provider's responsibility.
- **Interface** shall denote a communication session used by the account servicing payment service provider to provide standardized procedures, protocols and tools for interfacing and secure communication, as well as to exchange data for the purposes of providing payment services and monitoring payment transactions.

II. GENERAL AUTHENTICATION REQUIREMENTS

3. Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorized or fraudulent payment transactions for the purpose of the implementation of the security measures referred to in item 1 paragraph 1 indent 1 of this decision.

   The mechanisms referred to in paragraph 1 of this item shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalized security credentials.

4. Payment service providers shall ensure that the transaction monitoring mechanisms referred to in item 3 paragraph 1 of this decision, take into account, at a minimum, each of the following risk-based factors:
   - registered compromised or stolen authentication elements;
   - the amount of each payment transaction;
   - abnormal behavioral pattern of the payment service user or change in the direct access to the payment account, online (example: change in the usual access IP addresses or its rapid change in geographical location during one or more sessions, the so-called impossible travel, change of the payment device, atypical payments of the user to certain merchant categories, unusual payment transaction data);
   - known fraud scenarios in the provision of payment services;
   - signs of malware infection in any sessions of the authentication procedure;

III. SECURITY MEASURES FOR THE APPLICATION OF STRONG AUTHENTICATION

Authentication code

5. Payment service providers shall apply strong customer authentication, where the authentication shall be based on two or more elements which are categorized as knowledge (known only by the customer), possession (possessed only by the customer) and inherence (what the customer is) and shall result in the generation of an authentication code.

   The authentication code shall be only accepted once by the payment service provider for access to the payment account online, for initiating an electronic payment transaction or for

carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses.

6. For the purpose of item 5 hereof, payment service providers shall adopt security measures ensuring that each of the following requirements is met:
    - no information on any of the elements referred to in item 5 paragraph 1 can be derived from the disclosure of the authentication code;
    - it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;
    - the authentication code cannot be forged.

7. Payment service providers shall ensure that the authentication by means of generating an authentication code includes the following measures:
    - where the generating an authentication code has failed, it shall not be possible to identify which of the elements referred to in item 5 hereof was incorrect;
    - the number of failed authentication attempts that can take place consecutively, after which the access shall be temporarily or permanently hindered or blocked, shall not exceed five within a given period of time;
    - the communication session is protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorized parties in accordance with the requirements in Chapter V hereof;
    - the maximum time without activity by the payer after being authenticated shall not exceed 5 minutes.

8. Where the access hindering or block referred to in item 7 paragraph 1 indent 2 is temporary, the payment service provider shall establish the duration of that block and the number of retries based on the characteristics of the service provided to the payer and all the relevant risks involved, taking into account, at a minimum, the factors referred to in item 4 hereof.

   The payment service provider shall alert the payer that the electronic payment instrument is blocked before it is made permanent, or where that is not possible, immediately after the block.

   Where the block has been made permanent, the payment service provider shall establish a secure procedure to remove the block of the electronic payment instruments or to replace the blocked electronic payment instrument with a new one.

Dynamic linking

9. Where payment service providers apply strong customer authentication, in addition to the requirements of items 5, 6, 7 and 8 of this decision, they shall also adopt security measures that meet each of the following requirements:
    - the payer is made aware of the amount of the payment transaction and of the payee;
    - the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;

- the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;
- any change to the amount of the payment transaction or the payee results in the invalidation of the authentication code generated.

For the purpose of paragraph 1 of this item, payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:

- the amount of the transaction and the payee throughout all of the phases of the authentication;
- the information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code.

For the purpose of paragraph 1, indent 2 of this item and where payment service providers apply strong customer authentication, the following requirements for the authentication code shall apply:

- in relation to a card-based payment transaction for which the payer has given consent to the exact amount of the funds to be reserved, the authentication code shall be specific to the amount that the payer has given consent to the reservation when initiating the transaction;
- in relation to payment transactions for which the payer has given consent to execute a batch of electronic payment transactions to one or several payees, the authentication code shall be specific to the total amount of the batch of payment transactions and to the specified payees.

Requirements of the elements categorized as knowledge

10. Payment service providers shall adopt measures to mitigate the risk that the elements categorized as knowledge are uncovered by, or disclosed to, unauthorized parties.

    The use by the payer of the elements categorized as knowledge shall be subject to mitigation measures in order to prevent their disclosure to unauthorized parties.

Requirements of the elements categorized as possession

11. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorized as possession are used by unauthorized parties.

    The use by the payer of the elements categorized as possession shall be subject to measures designed to prevent replication of the elements.

Requirements of devices and software linked to elements categorized as inherence

12. Payment service providers shall adopt measures to mitigate the risk that the elements categorized as inherence and read by access devices and software provided to the payer are used by unauthorized parties.

The use by the payer of the elements categorized as inherence shall be subject to measures ensuring that those devices and the software guarantee resistance against unauthorized use of the elements through access to the devices and the software.

Independence of the elements

13. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in items 10, 11 and 12 hereof is subject to measures which ensure that the breach of one of the elements does not compromise the reliability of the other elements.

    Payment service providers shall adopt security measures, where any of the elements of strong customer authentication used or the authentication code generated through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.

    For the purposes of paragraph 2 of this item, payment service providers shall apply the following measures to mitigate the risk:

    - the use of separated secure execution environments through the software installed inside the multi-purpose device;
    - mechanisms to ensure that the software or device has not been altered by the payer or by a third party; and
    - where alterations to the software or the device have taken place, mechanisms to mitigate the consequences thereof.

IV. EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

Payment account information

14. Payment service providers shall be allowed to apply exemption from strong customer authentication, subject to compliance with the requirements laid down in item 4 hereof and where a payment service user is allowed a remote access to the payment account online, without disclosure of sensitive payment data, where there is a need of information about:
    - the balance of one or more designated payment accounts;
    - the payment transactions executed in the last 90 days through payment accounts designated by the user.

15. For the purpose of item 14 hereof, payment service providers shall not be exempted from the application of strong customer authentication where either of the following condition is met:
    - the payment service user is accessing online the information specified in item 14 hereof for the first time;
    - more than 90 days have elapsed since the last time the payment service user directly accessed online the information specified in item 14, paragraph 1, indent 2 hereof and strong customer authentication was applied.

Contactless payments at point of sale

16. Payment service providers shall be allowed to apply exemption from strong customer authentication, subject to compliance with the requirements laid down in item 4 hereof, where the payer initiates a contactless remote electronic payment transaction, provided that the following conditions are met:
    - the individual amount of the contactless remote electronic payment transaction does not exceed MKD 3000; and
    - the cumulative amount of previous contactless electronic payment transactions initiated by means of a payment instrument with a contactless functionality from the date of the last application of strong customer authentication does not exceed MKD 9000; or
    - the number of consecutive contactless electronic payment transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication does not exceed five.

Unattended terminals for transport fares and parking fees

17. Payment service providers shall be allowed to apply exemption from strong customer authentication, subject to compliance with the requirements laid down in item 4 hereof, where the payer initiates a remote electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

List of trusted beneficiaries

18. Payment service providers shall apply strong customer authentication where a payer creates or amends a list of trusted beneficiaries through the account servicing payment service provider.

    Payment service providers shall be allowed to apply an exemption from strong customer authentication, subject to compliance with the requirements referred to in item 4 thereof, where the payer initiates a payment transaction and the payee is included in the list referred to in paragraph 1 of this item.

Recurring transactions

19. Payment service providers shall apply strong customer authentication when a payer creates, amends, or initiates for the first time, a series of recurring electronic payment transactions with the same amount and with the same payee.

    Payment service providers shall be allowed to apply exemption from strong customer authentication, subject to compliance with the requirements laid down in item 4 hereof, for the initiation of all future payment transactions included in the subsequent series of payment transactions referred to in paragraph 1 of this item.

Credit transfers between accounts held by the same natural or legal person

20. Payment service providers shall be allowed to apply exemption from strong customer authentication, subject to compliance with the requirements laid down in item 4 hereof, where

the payer initiates a credit transfer in circumstances where the payer and the payee are the same natural person or legal entity and both payment accounts are held by the same account servicing payment service provider.

Low-value transactions

21. Payment service providers shall be allowed to apply exemption from strong customer authentication, where at the initiation of a remote electronic payment transaction, the following conditions are met:
    - the amount of the remote electronic payment transaction does not exceed MKD 1200; and
    - the cumulative amount of previous remote electronic payment transactions, initiated by the payer since the last application of strong customer authentication does not exceed MKD 6000; or
    - the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed five consecutive individual remote electronic payment transactions.

Secure corporate payment processes and protocols

22. Payment service providers shall be allowed to apply exemption from strong customer authentication, in respect of legal persons initiating electronic payment transactions through the use of dedicated payment processes or protocols that are only made available to payers who are not consumers, where those processes or protocols guarantee at least equivalent levels of security to those provided for by the Law.

Transaction risk analysis

23. Payment service providers shall be allowed to apply exemption from strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in item 4 paragraph 1 indent 4 of this decision.

    A payment transaction referred to in paragraph 1 of this item shall be considered as posing a low level of risk where all the following conditions are met:

    - the fraud rate for that type of transaction, calculated in accordance with item 24 and reported by the payment service provider is equivalent to or below the reference fraud rates specified in the table set out in the Annex 1 to this decision, for electronic card-based payments and electronic credit transfers, respectively;
    - the amount of the transaction does not exceed the relevant exemption threshold value specified in the table set out in Annex 1 to this decision;
    - payment service providers as a result of performing a real time risk analysis have not identified any of the following: abnormal payment or behavior of the payer; unusual information about the payer's device/software access; malware infection in any session of the authentication procedure; known fraud scenario in the provision of payment services; abnormal location of the payer; and high-risk domicile country of the payee.

Payment service providers that intend to exempt remote electronic payment transactions from strong customer authentication, on the ground of paragraph 2 of this item, shall take into account at a minimum, the following risk-based factors:

- the previous spending patterns of the individual payment service user;
- the payment transaction history of each of the payment service provider's payment service users;
- the location of the payer and the domicile country of the payee at the time of the remote payment transaction, in cases where the access device or software is provided by the payment service provider;
- the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be subject to strong customer authentication.

Calculation of fraud rates

24. The payment service provider shall, for each type of transaction referred to in the table set out in Annex 1 to this decision, ensure that the overall fraud rates covering both payment transactions authenticated through strong customer authentication and those executed under any of the exemptions referred to in items 18, 19, 20, 21, 22 and 23 of this decision, are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction indicated in the table set out in Annex 1 to this decision.

    The overall fraud rate for each type of transaction indicated in the table set out in Annex 1 to this decision, shall be calculated as the total value of unauthorized or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote electronic transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under any exemption referred to in items 18, 19, 20, 21, 22 and 23 of this decision.

    The calculation of the fraud rates referred to in paragraph 2 of this item shall be assessed by the audit review referred to in item 27 hereof, which shall ensure that they are complete and accurate.

    The methodology and any model, used by the payment service provider to calculate the fraud rates, as well as the fraud rates themselves, shall be adequately documented and made available to the National Bank, upon its request.

Cessation of exemptions based on transaction risk analysis

25. Payment service providers that make use of the exemption referred to in item 23 of this decision shall immediately report to the National Bank, where one of their monitored fraud rates, for any type of payment transactions indicated in the table set out in Annex 1 to this decision, exceeds the applicable reference fraud rate and shall provide a description of the measures that they intend to adopt to restore compliance of their monitored fraud rate with the applicable reference fraud rates.

Payment service providers shall immediately cease to make use of the exemption referred to in item 23 of this decision for any type of payment transactions indicated in the table set out in Annex 1 to this decision, in the specific exemption threshold range where their monitored fraud rate exceeds for two consecutive quarters the reference fraud rate applicable for that payment instrument or type of payment transaction in that exemption threshold range.

Following the cessation of the exemption referred to in item 23 of this decision and in accordance with paragraph 2 of this item, payment service providers shall not use that exemption again, until their calculated fraud rate equals to, or is below, the reference fraud rates applicable for that type of payment transaction indicated in the table set out in Annex 1 to this decision, in that exemption threshold range for one quarter.

Where payment service providers intend to make use again of the exemption referred to in item 23 of this decision, they shall notify the National Bank in a reasonable timeframe and shall before making use again of the exemption, provide evidence of the restoration of compliance of their fraud rate with the applicable reference fraud rate for that exemption threshold range in accordance with paragraph 3 of this item.

Monitoring

26. In order to make use of the exemptions set out in items 14, 15, 16, 17, 18, 19, 20, 21, 22 and 23 of this decision, payment service providers shall record and monitor the following data for both remote and non-remote payment transactions, at least on a quarterly basis:
    - the total value of unauthorized or fraudulent payment transactions, the total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions;
    - the average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions;
    - the number of payment transactions where each of the exemptions was applied and their percentage in respect of the total number of payment transactions.

    Payment service providers shall make the results of the monitoring in accordance with paragraph 1 of this item available to the National Bank, upon request.

Review

27. Payment service providers that make use of the exemption from strong customer authentication in accordance with item 23 of this decision shall be subject to an audit of the methodology, the model and the reported fraud rates.

    Payment service providers shall be subject to the audit referred to in paragraph 1 of this item during the first year of making use of the exemptions under item 23 of this decision and at least every 3 years thereafter, or more frequently at the National Bank's request.

V. CONFIDENTIALITY AND INTEGRITY OF THE USERS' PERSONALIZED SECURITY CREDENTIALS

General requirements

28. Payment service providers shall ensure the confidentiality and integrity of the personalized security credentials of the payment service user, including authentication codes, during all phases of the authentication.

    For the purpose of paragraph 1 of this item, payment service providers shall ensure that each of the following requirements is met:

    - personalized security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication;
    - personalized security credentials in data format, as well as cryptographic materials related to their encryption are not stored in plain text;
    - secret cryptographic material is protected from unauthorized disclosure.

    Payment service providers shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalized security credentials.

    Payment service providers shall ensure that the processing and routing of personalized security credentials and of the authentication codes generated in accordance with Chapter III of this decision take place in secure environments in accordance with strong and widely recognized industry standards adopted by international and European standardization organizations.

Creation and transmission of personalized security credentials

29. Payment service providers shall ensure that the creation of personalized security credentials is performed in a secure environment.

    Payment service providers shall mitigate the risks of unauthorized use of the personalized security credentials and of the authentication devices and software following their loss, theft or copying before their delivery to the payer.

Association with the payment service user

30. Payment service providers shall ensure that only the payment service user is associated, in a secure manner, with the personalized security credentials, the authentication devices and the software.

    For the purpose of paragraph 1 of this item, payment service providers shall ensure that each of the following requirements is met:

    - the association of the payment service user's identity with personalized security credentials, authentication devices and software is carried out in secure environments under the payment service provider's responsibility;

- the association by means of a remote channel of the payment service user's identity with the personalized security credentials and with authentication devices or software is performed using strong customer authentication.

Delivery of personalized security credentials, authentication devices and software

31. Payment service providers shall ensure that the delivery of personalized security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorized use due to their loss, theft or copying.

    For the purpose of paragraph 1 of this item, payment service providers shall at least apply each of the following measures:

    - effective and secure delivery mechanisms ensuring that the personalized security credentials, authentication devices and software are delivered to the legitimate payment service user;
    - mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user by means of the Internet;
    - arrangements ensuring that, where the delivery of personalized security credentials is executed outside the premises of the payment service provider or through a remote channel: no unauthorized party can obtain more than one feature of the personalized security credentials, the authentication devices or software when delivered through the same channel; the delivered personalized security credentials, authentication devices or software require activation before usage;
    - arrangements ensuring that, in cases where the personalized security credentials, the authentication devices or software have to be activated before their first use, the activation shall take place in a secure environment in accordance with the association procedures referred to in item 30 of this decision.

Renewal of user's personalized security credentials

32. Payment service providers shall ensure that the renewal or reactivation of user's personalized security credentials adhere to the procedures for the creation, association and delivery of the user's personalized security credentials and of the authentication devices as defined in items 29, 30 and 31 of this decision.

Destruction, deactivation and revocation

33. Payment service providers shall ensure efficient processes in place to apply the following security measures:
    - secure destruction, deactivation or revocation of user's personalized security credentials, authentication devices and software;
    - where the payment service provider distributes reusable authentication device and software, before reuse by another payment services user, secure reuse of the device or software shall be established, documented and implemented;

- deactivation or revocation of information related to user's personalized security credentials stored in the systems and databases of payment service providers and, depending on the cases, in other public repositories.

VI. COMMON, SECURE AND OPEN STANDARDS OF COMMUNICATION

General requirements for communication identification

34. Payment service providers shall ensure secure identification when communicating between the payer's device and the recipient's acceptance device for electronic payments, including payment terminals.

    Payment service providers shall ensure effective mitigation of the risk of misdirection of communication to unauthorized parties in mobile applications and other payment service users' interfaces that offer payment services.

General requirements for payment transactions monitoring

35. Payment service providers shall establish procedures that ensure monitoring of all payment transactions and other interactions between the payment service user, other payment service providers and entities, including merchants, in the provision of payment services and shall provide information on all significant events for electronic payment transactions in all stages of their execution and their availability after the execution of the transactions.

    For the purposes of paragraph 1 of this item, payment service providers shall ensure that every communication session established with the payment service user, other payment service providers and entities, including merchants, contains the following:

    - a unique identifier of the session;
    - detailed logging of the transaction, including transaction number, electronic timestamps and all relevant transaction data.

Specific requirements for the common, secure and open standards of communication

Access interfaces

36. Account servicing payment service providers that offer to a payer a payment account that is accessible directly, online, shall have in place at least one interface which meets each of the following requirements:

    - account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments are able to identify themselves towards the account servicing payment service provider;
    - account information service providers are able to communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions;
    - payment initiation service providers are able to communicate securely to initiate a payment order from the payer's payment account, receive feedback information on the initiation of the payment transaction and all information regarding the execution

of the payment transaction accessible to the account servicing payment service providers.

37. For the purposes of authentication of the payment service user, the interface referred to in item 36 of this decision shall allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user.

    The access interface shall meet at least the following requirements:

    - based on the consent of the payment service user, a payment initiation service provider or an account information service provider shall be able to instruct the account servicing payment service provider to start the authentication;
    - communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and any payment service user concerned shall be established and maintained throughout the authentication;
    - integrity and confidentiality of the personalized security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider shall be ensured.

38. Account servicing payment service providers shall ensure to harmonize their interfaces with the data structure standards and their models, application, transport and authorization level protocols, using widely accepted industry standards adopted by international or European standardization authorities.

    Account servicing providers shall provide technical specification of its interfaces, specifying a set of routines, protocols and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments for ensuring interoperability between own systems with the systems of the account servicing payment service providers.

    Account servicing payment service providers, upon request of payment initiation service providers, account information service providers, payment service providers issuing card-based payment instruments registered in the payment institutions registry or payment service providers that have applied to their competent authorities for the relevant authorizations shall make the documentation of paragraph 2 of this item publicly available free of charge and publish a summary of the documentation on their website, at least five months before the date of application specified in item 67 of this decision or before the scheduled date of interface introduction, if the interface introduction date is after the date specified in the same item.

39. Account service providers shall ensure all changes in the technical documentation for their interfaces to be available to the payment initiation service providers, account information service providers, payment service providers issuing card-based payment instruments registered in the payment institutions registry or payment service providers that have applied for obtaining a license for providing payment services, except in emergency situations.

    The change in the interface technical documentation shall be available as soon as possible, at least three months before the change is implemented.

Payment service providers, in case of interface changes imposed by emergency situations shall document the actions and submit to the National Bank upon request.

40. Account service providers shall ensure testing facility and assistance in order to test the connection and functionalities of the software and applications of payment initiation service providers, account information service providers, payment service providers issuing card-based payment instruments registered in the payment institutions registry or payment service providers that have applied for obtaining a license for providing payment services, except in emergency situations.

    The testing facility shall be available at least five months before the date of application specified in item 67 of this decision or before the scheduled date of interface introduction, if the interface introduction date is after the date specified at the same item.

    No sensitive information shall be shared through the testing facility.

Utilization of interfaces

41. Account servicing payment service providers shall establish interface, in conformity with the requirements referred to in items 36, 37,38, 39 and 40 of this decision by:
    - providing a dedicated interface or
    - using the interface of the payment service providers referred to in item 36 of this decision, which is applied for authentication and communication with the payment service users it ensures.

Requirements for dedicated interface

42. Provided that the requirements referred to in items 36, 37, 38, 39, 40 and 41 of this decision are met, account servicing payment service providers that have established a dedicated interface shall ensure the same level of availability, efficiency, including support, as well as for the interface used to access account servicing payment service users, directly, online.

43. Account servicing payment service providers, who have established a dedicated interface, shall define transparent key indicators of efficiency and target level of services, which also in terms of availability and exchanged data in accordance with items 62, 63, 64, 65 and 66 of this decision, shall be as strict as those for the interface used by their payment service users.

    When monitoring the level of services, availability and efficiency, account servicing payment service providers shall adhere to the guidelines given in Annex no. 2 of this decision.

44. Account servicing payment service providers that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services.

    As obstacles of paragraph 1 of this item shall be considered the following instances:

    - when the payment service providers referred to in item 36 of this decision do not have the possibility to use the user personalized security credentials, which the account servicing payment service providers have provided to their users;
    - requests for authentication;

- requests for additional verification of the licenses entered in the payment institutions registry;
- additional verification of the consent given by payment service users to providers of payment initiation and account information services.

The account servicing payment services provider shall, at the request of the National Bank, submit a report that the dedicated interface does not create an obstacle in the providing of payment initiation and account information services in accordance with the guidelines of Annex no. 5 of this decision.

45. For the needs of items 42 and 43 of this decision, the account servicing payment service providers shall monitor the availability and efficiency of the dedicated interface.

    Account servicing payment service providers shall publish on their website quarterly statistics on the availability and efficiency of the dedicated interface and of the interface used by its payment service users.

    When publishing the statistics on the availability and efficiency of the dedicated interface and of the interface used by its payment service users, the account servicing payment service providers shall adhere to the guidelines provided in Annex 3 of this decision.

46. Account servicing payment service providers shall conduct stress testing to the resilience of the dedicated interface, in accordance with the guidelines provided in Annex 4 of this decision.

    As part of the stress-testing of the resilience, the account servicing payment service providers shall determine the impact they have on the availability and efficiency of the dedicated interface and the defined level of service.

    Account servicing payment service provider shall at the request of the National Bank, submit a summary report of the results of the latest stress-testing of the resilience, as well as information on the ways in which the identified weaknesses were overcome.

Standards for dedicated interface continuity and conditions for facilitated implementation

47. Account servicing payment service providers, in designing the dedicated interface, shall include continuity standards, by developing a strategy, continuity plans, in the event that the dedicated interface does not function in accordance with the requirements referred to in items 42, 43, 44, 45 and 46 of this decision, that is, in case of unplanned unavailability or a system breakdown.

    Unplanned unavailability or a systems breakdown may be presumed to have arisen when five consecutive requests for access to information for the provision of payment initiation services or account information services are not replied to within 30 seconds.

48. The business continuity plan shall describe the communication method to inform the payment service providers using the dedicated interface, about the measures to restore the systems and a description of the immediately available alternative options payment service providers may have.

49. Account servicing payment service providers and payment service provided referred to in item 36 of this decision shall report without delay the problems that arise with the dedicated interface, specified in item 47 of this decision and the information related to overcoming the problems in accordance with the guidelines in Annex 8 of this decision, to the National Bank.

50. As part of the continuity standards, for functioning in emergency situations, payment service providers referred to in item 36 of this decision may use the interfaces made available to payment service users for authentication and communication with the account servicing payment service provider, until the required level of availability and efficiency of the dedicated interface is ensured according to items 42 to 46 of this decision.

51. For the purposes of item 50 of this decision, the account servicing payment service providers shall ensure that the payment service providers referred to in item 36 of this decision shall identify themselves with the authentication procedures that the account servicing payment service providers ensure to the payment service users.

    If the payment service providers referred to in item 36 of this decision use the interface referred to in item 50 of this decision, they shall:

    - take necessary measures ensuring that they do not access, store or process data for purposes other than providing the service requested by the payment service users;
    - continue to fulfill legal requirements concerning the payment account access rules in case of initiating a payment and receiving information about the payment account;
    - record data that is accessed through the interface that the account servicing payment service provider maintains for the needs of its payment service users and at the request and without delay, to submit the data records to the National Bank;
    - at the request of the National Bank and without undue delay, to explain the way of using the interface that is given to the payment service users when accessing their payment account, directly, online;
    - inform the account servicing payment service providers in an appropriate manner.

52. If the account services payment service providers have decided to use a dedicated interface with simplified application of continuity standards, for which requirements referred to in item 50 of this decision do not apply, they should fulfill the following:
    - compliance with the dedicated interface requirements referred to from item 42 to item 46 of this decision;
    - that the dedicated interface is designed and tested in accordance with the requirements referred to in item 40 of this decision;
    - the dedicated interface has been widely used by account information payment service providers, initiating payments and confirming available funds for payment card payments, for a period of at least three months;
    - all problems that have arisen in the functioning of the dedicated interface have been overcome without undue delay.

    Account servicing payment service providers shall at a request of the National Bank ensure a confirmation for the fulfillment of the requirements referred to in paragraph 1 of this item, in accordance with the guidelines in Annex 6, Annex 7 and Annex 8 of this decision.

53. If the account servicing payment service providers do not fully comply with the requirements of item 52 for a period of more than two consecutive calendar weeks, they shall, as soon as

possible, but no later than two months, establish procedures for the application of the continuity standards referred to in item 50 of this decision.

Certificates

54. For the purpose of authentication referred to in item 36 paragraph 1 indent 1 of this decision, the payment service providers shall use qualified certificates for electronic seals or qualified certificate for website authenticity in conformity with the Law on Electronic Documents, Electronic Identification and Trust Services.

55. The qualified certificates for electronic seals or for website authentication referred to in item 54 of this decision shall include, in a language customary, the specific attributes in relation to each of the following items:
    - a type of payment service provider that can have one or more of the following roles: account servicing; payment initiation; account information; issuing of card-based payment instruments;
    - registration number of the payment service provider in the register of payment institutions and name of the competent authority where the payment service provider is registered.

56. The attributes referred to in item 55 of this decision shall not affect the interoperability and recognition of the qualified certificates for electronic seals or the website authenticity.

Security of communication session

57. Account servicing payment service providers, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers, when exchanging data by means of the internet between all communicating parties throughout the respective communication session shall apply secure encryption by using widely recognized industrial standards, in order to safeguard the confidentiality and the integrity of the data.

58. Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the access sessions offered by account servicing payment service providers as short as possible and they shall actively terminate any such session as soon as the requested action has been completed.

59. In case of parallel communication sessions with the account servicing payment service provider, the payment initiation service providers and account information service providers shall ensure that they are securely linked to relevant relevant established with the payment service users in order to prevent the possibility that any message or information communicated between them could be misrouted.

60. In the communication with the account servicing payment service provider, the account information service providers, the payment initiation service provider and the payment service providers issuing card-based payment instruments shall ensure the following elements:

- payment service users and corresponding communication session, in order to distinguish several requests from the same payment service users;
- for payment initiation services, the uniquely identified payment transaction initiated;
- for confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of the card-based payment transaction.

61. Account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall ensure that when communicating the personalized security credentials and authentication codes, they not be readable, directly or indirectly, by any staff at any time.

    In case of loss of confidentiality of personalized security credentials within the competence of the payment service providers referred to in paragraph 1 of this item, they shall inform, without undue delay, the payment service user and the issuer of the personalized security credentials.

Data exchanges

62. Account servicing payment service providers shall comply with the following requirements:
    - they shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user online, provided that this information does not include sensitive payment data;
    - they shall, immediately after receipt of the payment order, provide payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the latter;
    - they shall, upon request, immediately provide payment service providers with a confirmation in a simple 'yes' or 'no' format, whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer.

63. In case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements, the account servicing payment service provider shall send a notification message to the payment initiation service provider or the account information service provider and the payment service provider issuing card-based payment instruments which explains the reason for the unexpected event or error.

    If the account servicing payment service provider offers a dedicated interface in accordance with items 42, 43, 44, 45 and 46 of this Decision, the interface shall provide for notification messages concerning events from paragraph 1 of this item to be communicated by the payment service provider that detected the events to the other payment service providers participating in the communication session.

64. Account information service providers shall have in place suitable and effective mechanisms that prevent access to information other than from designed payment accounts and associated payment transactions, in accordance with the user's consent.

65. Payment initiation service providers shall provide account servicing payment service providers with the same information as requested from the payment service user when initiating the payment transaction directly.

66. Account information service providers shall be able to access information from designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of performing the account information service in either of the following circumstances:
    - whenever the payment service user is actively requesting such information;
    - where the payment service user does not actively request such information, no more than four times in a 24-hour period, unless a higher frequency is agreed between the account information service provider and the account servicing payment service provider, with the payment service user's consent.

VII. TRANSITIONAL AND CLOSING PROVISIONS

67. The payment service providers that are founded up to the date this Decision becomes applicable shall comply their operations with the requirements of this Decision not later than 19 February 2024.

    Notwithstanding paragraph 1 of this item, payment service providers that are founded up to the date this Decision becomes applicable and are account servicing, shall:

    - make available a testing facility and support, for connection and functional testing of dedicated interface in accordance with item 40 of this Decision and evidence of compliance with the requirements regarding the design of the dedicated interface and aggregated test results, in accordance with Annex no. 6, enclosed in this decision, at least five months before the date for its operation compliance with the requirements set out in this Decision, no later than 30 September 2023;
    - submit report that the dedicated interface does not create obstacles to the provision of payment initiation and account information services, at least two months before the date for its operation compliance with the requirements set out in this Decision, no later than 31 December 2023;
    - submit summary of the results of the resilience stress-testing, as well as specify how the identified weaknesses have been solved, at least one month before the date of its compliance with the requirements set out in this Decision, no later than 31 January 2024.

68. This decision shall enter into force on the eighth day of its publication in the Official Gazette of the Republic of North Macedonia.

D no. 02-15/XXII-7/2022
28 December 2022
Skopje

Anita Angelovska Bezhoska
Governor and Chairperson
of the Council of the National Bank
of the Republic of North Macedonia

ANNEXES:

ANNEX 1	-	Reported fraud rates
ANNEX 2	-	Availability and performance monitoring of the dedicated interface
ANNEX 3	-	Publishing statistical data
ANNEX 4	-	Resilience stress-testing
ANNEX 5	-	Obstacles
ANNEX 6	-	Design and testing of the dedicated interface
ANNEX 7	-	Wide usage of dedicated interface
ANNEX 8	-	Resolution of problems

ANNEX 1
Reported fraud rates

Reported fraud rates in %		
Exemption threshold value (in denars)	Electronic card-based payment transactions	Electronic credit transfers
up to 30,000	0.01	0,005
up to 15,000	0.06	0.01
up to 6000	0.13	0,015

ANNEX 2

Availability and performance monitoring of the dedicated interface

1. For the needs of availability and performance monitoring of the dedicated interface, account servicing payment service providers shall define at least the following key indicators:
    - Dedicate interface uptime per day;
    - Dedicated interface downtime per day;
    - Daily average payment initiation time;
    - Daily average time for providing account information;
    - Daily average time to provide, upon request, the card-based payment instrument issuer with a confirmation in a simple "yes" or "no" format;
    - Daily error response rate.

2. To calculate the availability and efficiency indicators of dedicated interface from item 1 of this Annex, account servicing payment service providers shall:
    - Calculate the uptime as 100% minus the percentage of downtime;
    - Calculate the percentage downtime, using the total number of seconds the dedicated interface was down defined in item 3 of this Annex in a 24-hour period (in seconds) starting and ending at midnight;
    - Calculate the average daily payment initiation time (in milliseconds) as total information submission time in accordance with item 62 paragraph 1 indent 1 of this Decision, per request in a 24-hour period, starting and ending at midnight;
    - Calculate the account information service provider average daily time(in milliseconds) as a total informing time in accordance with item 62 paragraph 1 indent 1 of this Decision, per request in a 24-hour period, starting and ending at midnight;
    - Calculate the average daily time to provide, upon request, the card-based payment instrument issuer (in milliseconds) with a confirmation in a simple "yes" or "no" format as a total information submission time in accordance with item 62 paragraph 1 indent 3 of this Decision, per request in a 24-hour period, starting and ending at midnight.
    - Calculate the daily error response rate as number of daily error messages sent by the account servicing payment service provider to payment initiation service providers, account information service providers and card-based payment instrument issuers by total daily number of requests by the aforementioned providers.

3. The dedicated interface shall count as down when five consecutive services for payment initiation, account information or confirmation of availability of funds are not replied to within 30 seconds, irrespective of whether these requests originate from one or multiple payment initiation service providers, account information service providers and card-based payment instrument issuers.

   Account servicing payment service provider shall calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided.

ANNEX 3

Publishing statistical data

1. Account servicing payment service provider shall disclose the quarterly statistics on availability and efficiency of dedicated interface on its website, for the payment service users to directly access their accounts, online.

2. With the plan disclosure, the account servicing payment service provider lists the website for statistical data reporting, as well as the data of their initial publishing.

3. Payment initiation service providers, account information service providers and card-based payment instrument issuers use these statistical data on daily basis to compare the availability and efficiency of dedicated interface to the availability and efficiency of interfaces provided by account servicing payment service providers for the payment service users to directly access their accounts online.

ANNEX 4

Resilience stress-testing

1. Account servicing payment service provider shall conduct an adequate stress-testing of the dedicated interface resilience, every three years, in terms of:
    - its ability to provide access to multiple payment initiation service providers, account information service providers and card-based payment instrument issuers,
    - its ability to process, in a short time period, an extremely high number of requests that originate from initiation service providers, account information service providers and card-based payment instrument issuers;
    - its services used by an extremely high number of communication channels for payment initiation, account information and confirmation on availability of funds, put in place at the same time; and
    - its ability to meet the requirements for large amount of data.

ANNEX 5

Obstacles

1. Account servicing payment service provider shall prepare a report that the dedicated interface does not create obstacles, which contains:
    - a summary of methods of carrying out the authentication procedures of the payment service users that are supported by the dedicated interface i.e. redirection, decoupled, and embedded or a combination thereof.
    - an explanation of the reasons why the methods of carrying out the authentication procedures are not an obstacle and on the basis of which payment initiation service providers and account information service providers can rely on the authentication procedures provided by the account servicing payment service provider to its payment service users.
    - confirmation that dedicated interface does not give rise to unnecessary delay or friction in the experience available to the payment service users when accessing their account via a payment initiation service providers, account information service providers or card-based or card-based payment instrument issuers or to any other attributes, including unnecessary or superfluous steps or the use of unclear or discouraging language, that would directly or indirectly dissuade the payment service users from using the services of payment initiation service providers, account information service providers or card-based payment instrument issuers.

2. As part of the explanation of item 1 paragraph 1 indent 2 of this Annex, the account servicing payment service provider shall provide the competent authority with a confirmation that:
    - the dedicated interface does not prevent payment initiation service providers, account information service providers from relying upon the authentication procedures provided by account servicing payment service provider to its payment service users;
    - no additional authorizations or registrations are required from payment initiation service providers, account information service providers or card-based payment instrument issuers;
    - there are no additional checks by the account servicing payment service provider on the consent given by the payment service user to the payment initiation service provider or account information service provider to access the information on the payment accounts held with the account servicing payment service provider or to initiate payments; and
    - no checks on the consent given by payment service user to card-based payment instrument issuers were performed, for confirmation of availability of funds.

ANNEX 6

Design and testing of the dedicated interface

1. For the purpose of evidencing compliance with the requirement regarding the design of the dedicated interface, the account servicing payment service provider should provide the National Bank with:
    - evidence that the dedicated interface meets the legal requirements for access and data, including: a description of the functional and technical specifications and a summary of how the implementation of these specifications fulfills the requirements and
    - information on whether, and if so how, the account servicing payment service provider has engaged with payment initiation service providers, account information service providers and card-based payment instrument issuers.

2. Regarding the testing of the dedicated interface, the account servicing payment service provider should make the technical specifications of the dedicated interface available to authorized payment initiation service providers, account information service providers and card-based payment instrument issuers or payment service providers that have applied to their competent authorities for the relevant authorization.

3. The testing facility shall allow account servicing payment service providers, payment initiation service providers, account information service providers, card-based payment instrument issuers registered in the payment institutions registry or payment service providers that have applied to their competent authorities for the relevant authorizations to test the dedicated interface in a secure, dedicated testing environment with non-real payment service users data, for the following:
    - a stable and secure connection;
    - the ability of account servicing payment service providers, and authorized payment initiation service providers, account information service providers and card-based payment instrument issuers registered in the payment institutions registry to exchange the relevant certificates;
    - the ability to send and receive error messages;
    - the ability of payment initiation service providers to send, and of account servicing payment service providers to receive, payment initiation orders and the ability of account servicing payment service providers to provide the information requested;
    - the ability of account information service providers to send, and of account servicing payment service providers to receive, requests for access to payment account data, and the ability of account servicing payment service providers to provide the information requested;
    - the ability of card-based payment instrument issuers and payment initiation orders to send, and of account servicing payment service providers to receive, requests from card-based payment instrument issuers and payment initiation service providers and the ability of the account servicing payment service provider to send a "yes/no" confirmation to card-based payment instrument issuers and payment initiation orders;

- the ability of payment initiation service providers and account information service providers to rely on all the authentication procedures provided by the account servicing payment service provider to its payment service users.

4. The account servicing payment service provider should provide the National Bank with a summary of the results of the testing referred to in item 3 of this Annex for each of the elements to be tested, including the number of payment initiation service providers, account information service providers and card-based payment instrument issuers that have used the testing facility, the feedback received by the account servicing payment service provider from these payment initiation service providers, account information service providers and card-based payment instrument issuers, the issues identified and a description of how these issues have been addressed.

ANNEX 7

Wide usage of dedicated interface

1. For the purpose of evidencing wide usage of the dedicated interface, account servicing payment service provider shall provide the

   National Bank with:
   - a description of the usage of the dedicated interface for a period of at least three months, including: the number of payment initiation service providers, account information service providers and card-based payment instrument issuers that have used the interface and the number of requests sent by those providers via the dedicated interface that have been replied to by the account servicing payment service;
   - evidence that the account servicing payment service provider has made all reasonable efforts to ensure wide usage of the dedicated interface, including by communicating its availability and efficiency statistics via websites and social media.

ANNEX 8

Resolution of problems

1. For the purpose of evidencing measures taken for resolution of problems related to dedicated interface, account servicing payment service providers shall provide the National Bank with:
    - information on the systems or procedures in place for tracking, resolving and closing problems, particularly those reported by payment initiation service providers, account information service providers and card-based payment instrument issuers; and
    - an explanation of the problems reported by those providers in paragraph 1, indent 1of this item that have not been resolved in accordance with the service levels.