Pursuant to Article 47, paragraph 1, item 6 of the Law on the National Bank of the Republic of Macedonia ("Official Gazette" no. 158/10 and 123/12) and Article 27-b paragraph 6 of the Law on Payment Operations ("Official Gazette of the Republic of Macedonia" No. 113/07, 22/08, 159/08, 133/09, 145/10, 35/11, 11/12, 59/12 and 166/12), the National Bank of the Republic of Macedonia Council adopted the following

DECISION
on the technical standards
for performing micropayments
("Official Gazette of the Republic of Macedonia" no. 50/13)

I. GENERAL PROVISIONS

1. This Decision sets forth the technical standards which the intermediary in micropayments shall meet.

Technical standards include the criteria for ensuring the reliability and availability of the established operational information system, reliable and efficient transfers of funds between the user of the micropayment, the intermediary in the micropayment and the suppliers of products and services in the micropayment.

2. Certain terms used in this decision shall have the following meanings:

2.1. Participants in the micropayment system shall be: micropayment users and suppliers of products and services who have concluded contracts with the intermediary in micropayments.

2.2. The information system that is used for processing the micropayments (hereinafter: micropayment information system) shall include the information system located with the intermediary in micropayment, the telecommunications connection and the information point of presence with the service supplier.

2.3. Means of information shall be the parts of the micropayment information system that keep, pass and change the information that is transmitted through the micropayment information system.

2.4. Information point of presence with the products and services supplier (hereinafter: point of presence) shall denote the specialized hardware terminal equipment or specialized software infrastructure through which the micropayment users begin and confirm the micropayment by the means of telecommunication, the digital and information-technological devices. The micropayment user may have one or more means of telecommunication and/or digital-technological devices through which they may be connected to the micropayment information system through the information point of presence with the supplier of products and services. With these

tools/devices the micropayment user may start and may issue a consent for performing a micropayment.

2.5. Physical point of presence with the supplier of products and services shall denote the installation of a specialized terminal equipment with the supplier of products and services.

2.6. Virtual point of presence shall denote the installation of a specialized software infrastructure with the supplier of products and services through which the micropayment user may begin and confirm the micropayment.

2.7. Verification of the identity of the micropayment user shall denote a system for a single identification and verification of the identity of the micropayment user.

2.8. Double verification of the identity of the micropayment user shall denote a system for a single identification and verification of the identity of the micropayment user which takes place through two independent lines/channels of access to the micropayment information system.

2.9. Information system security shall denote the establishment and application of technical standards for information system security through risk analysis, information system security policy and verification of the user identity.

2.10. Confidentiality of the micropayment information system shall denote the availability of information and information means depending on the degree of confidentiality, to the persons who have authorized access.

2.11. Integrity of the micropayment information system shall denote protection of the accuracy and completeness of information transmitted through the information means.

2.12. Risk to the security of the micropayment information system shall denote the risk of financial loss or damaged reputation for the intermediary in micropayment due to loss and unauthorized use of information and information means.

2.13. Operational availability shall denote the performance of operational activities in accordance with performance indicators defined for the micropayment information system.

2.14. Safe and efficient transfer of funds shall denote the transfer of funds in accordance with the rules for the manner of processing, liability and return, settlement, limits control and transparency of the micropayment system, contained in this Decision.

2.15. Outsourcing company for the micropayment information system (hereinafter: outsourcing company) shall denote a third person, who on the basis of a written contract, collects, processes and stores data for the intermediary in micropayment while performing micropayments.

II. TECHNICAL STANDARDS FOR MICROPAYMENT INFORMATION SYSTEM SECURITY

Risk analysis

3. For the purpose of this Decision, risk analysis shall denote establishing a permanent process of assessing the risks to the micropayment information system security.

The process shall include:
- Identification of information and information means of the micropayment information system;
- Classification of information and information means of the micropayment information system in terms of their level of confidentiality and integrity;
- Analysis of the likelihood of adverse events and vulnerabilities of the micropayment information system and identification of possible consequences;
- Assigning priority of risks depending on the size of the potential financial loss or reputation damage they may cause.

The intermediary in micropayment shall be obliged to prepare a report on the risks analysis.

The intermediary in micropayment shall be obliged to perform risk analysis at least before each change in the established micropayment information system.

Information System Security Policy

4. The intermediary in micropayment shall adopt and apply an Information System Security Policy, which shall include at least the following elements:
- Classification of information and information means with a degree of confidentiality;
- Conduct of risk analysis;
- Manner of informing the micropayment user and the supplier of products and services about the proper use of the system;
- Definition of the procedure for developing, maintaining and blocking the mechanisms for providing verification of the micropayment user identity;
- Definition of the procedure for preparing, maintaining and withdrawing the hardware/software infrastructure intended for the suppliers of products and services;
- Management of security incidents and establishment of an appropriate mechanism for their identification, reporting and effective removal of possible risks to the micropayment information system security;
- Definition of an appropriate documented procedure for recording the proceedings and order of operations performed on certain parts of the micropayment information system;
- Definition of the manner of telecommunication connection and providing protection of the data that are transferred at different levels of the micropayment information system;
- Definition of security zones to restrict physical access to important information and information means from the micropayment information system;
- Description of the established administrative, technical and physical security controls in the micropayment information system.

The intermediary in micropayment may establish appropriate internal regulations for the effective implementation of the Policy from paragraph 1 of this item.

5. The intermediary in micropayment shall notify the National Bank of the Republic of Macedonia (hereinafter: the National Bank) in cases when they identify the highest level of security incident in the micropayment information system.

The intermediary in micropayment shall submit the notification referred to in paragraph 1 of this item to the National Bank, in a period no longer than three days from the date the security incident occurred.

Verification of the micropayment user identity

6. The intermediary in micropayment shall define and apply safe and effective methods for verifying the identity of the micropayment user. Mechanisms for identity verification shall be developed in an appropriate environment with limited access.

7. Verification of the identity of the micropayment user may be made by using the following three methods:
- By a syllable of characters known only to the micropayment user such as password, permanent PIN, single purpose PIN, etc.;
- By means of telecommunication, digital and technological devices that only the micropayment user possesses, such as mobile phone, digital tuner, e-card, and the like, and/or
- Through some of the unique personal physical characteristics of the micropayment user, such as fingerprint, voice recognition, etc.

8. Verification of the micropayment user's identity with a combination of at least two of the three methods defined in item 7 of this Decision shall be incorporated in the micropayment information system.

9. The verification of the micropayment user's identity is conducted through the point of presence with the supplier of products and services by using an encrypted telecommunications channel to the micropayment information system.

10. If the intermediary in micropayment makes double verification of identity through preparation of a syllable of characters that will be used for only one purpose in real-time execution of the micropayment, they may submit it to the micropayment user in an unencrypted form.

11. If the connection of the device of item 7, paragraph 1, indent 2 of this Decision with the point of presence with the supplier of products and services is conducted in a contactless manner, it should be protected by appropriate encryption.

12. The micropayment user and the supplier of products and services shall transfer the information on the amount of the micropayment from the point of presence with the supplier of products and services to the information system located with the intermediary in micropayment in an unreadable form, with an appropriate level of protection depending on the degree of confidentiality of the classified information and an appropriate level of protection of their integrity.

Use of outsourcing companies in the micropayment information system

13. Prior to the selection of the outsourcing company, the intermediary in micropayment shall analyze the risks to its operations that may result from the use of the outsourcing services.

14. A contract shall be concluded with the outsourcing company, which shall govern at least the elements set out in item 4 of this Decision, including the following safeguards: clause for information non-disclosure, clause for the level of service quality, key performance indicators, clause for coordinated security incidents management, clause defining the responsibility in case of complaints and returns.

The intermediary in micropayment shall not enter into a contract with the outsourcing company if the contract in any way prevents, limits or impedes the access of the National Bank during the supervision, in accordance with the Law on Payment Operations.

15. The operation of the outsourcing company shall be aligned with the information system security policy stipulated under item 4 of this Decision.

III. TECHNICAL STANDARDS FOR OPERATIONAL AVAILABILITY

Performance Indicators

16. The intermediary in micropayment shall define, determine and apply performance indicators for the operational availability of the established micropayment information system.

17. The intermediary in micropayment shall monitor the established indicators through regular reports on operational availability.

Operational capacity of the micropayment system

18. The intermediary in micropayment shall provide adequate capacity of the established micropayment information system. The capacity shall be planned taking into account also the assumed scenarios for a significant increase of the participants in the system and the number of processed micropayment orders, while meeting the performance indicators defined by item 16 of this Decision.

19. The plans for the needed capacity shall provide storage of archived data within the legally established timeframes.

IV. TECHNICAL STANDARDS FOR SAFE AND EFFICIENT TRANSFER OF FUNDS

Processing

20. Processing of a micropayment order means submission of a micropayment order to the information system located with the micropayment intermediary, by using the means of telecommunication, digital and information-technological devices by the micropayment user at the point of presence with the supplier of products and services.

21. The intermediary in micropayment shall inform the micropayment user and the supplier of products and services on the status of the processed micropayment order and the amount of the micropayment in accordance with the defined performance indicators.

22. The intermediary in micropayment shall define and provide a procedure for canceling the processed micropayment order with the supplier of products and services.

23. The intermediary in micropayment shall store and archive the processed orders for executed micropayments within the timeframes set in accordance with the internal regulations.

24. The intermediary in the micropayment shall define by an internal act the procedures for timely completion of the processing in case of technical problems in the processing and settlement of micropayments.

Responsibilities and Returns

25. The rights and responsibilities of the participants in the micropayment system shall be specified in the contracts between the intermediary and the participants in the system.

26. The intermediary in micropayment shall inform the micropayment users through a manual prepared in writing which shall contain:
- Definition of the procedures for conducting safe micropayments and
- Description of the best practices for avoiding adverse events and risks inherent in the established micropayment information system.

27. The intermediary in micropayment shall have a defined procedure for complaint and cancellation of the processed micropayment order by a participant in the micropayment system.

28. The processed micropayment order cannot be cancelled, if accepted as provided in item 20 of this Decision.

29. The intermediary in micropayment shall provide a 24-hour technical support to enable blocking of the means of telecommunication, digital and information-technological devices, and points of presence, if requested by their customers. The sequence of actions and activities that are performed by the persons employed in technical support shall be part of the recording system in accordance with item 4 paragraph 1 indent 7 of this Decision.

30. Upon receipt of a blocking notice from a micropayment user, processed micropayment orders shall be borne by the intermediary in micropayment.

31. In case of failure of certain parts of the micropayment information system, and processing of a single order multiple times, the responsibility shall be on the part of the intermediary in micropayment. If the intermediary in micropayment uses an outsourcing company for the micropayment information system, the responsibility shall be on the part of the intermediary in micropayment.

32. If the micropayment user fails to take steps to timely block the means of telecommunication, digital or information-technological device as required by the intermediary in micropayment, the responsibility shall be on the part of the micropayment user.

Settlement

33. The intermediary in micropayment shall provide compulsory settlement of processed micropayment orders through one of the registered systems for payment, clearing and settlement in the Republic of Macedonia.

34. The settlement of processed micropayment orders between the suppliers of products and services and the intermediary in micropayment shall not be longer than one working day after the end of the current cycle of calculation, as defined in the Law on Payment Operations.

Limits control

35. The intermediary in micropayment shall provide a system for control of the defined limits for micropayment in one cycle of calculation, as well as an automated reporting system on the fulfillment of the prescribed limits pursuant to the Law on Payment Operations.

36. The intermediary in micropayment shall not process the micropayment orders within the cycle of calculation, if the amount of micropayment exceeds the amount prescribed by the Law on Payment Operations. The intermediary in micropayment shall not process the micropayment order if with the processing of the order the monthly limit per intermediary in micropayment or the limit on micropayment user within the cycle of calculation, are exceeded.

37. The intermediary in micropayment shall inform the participants about the reason why the processing of the micropayment order was rejected.

Transparency

38. The micropayment users and the supplier of products and services shall be timely informed about the costs of using, maintaining and canceling the services of the intermediary in micropayment.

39. The intermediary in micropayment shall publicly disclose:
- The guidelines for users and micropayment
- The price list for the services and costs of performing the micropayment for the micropayment users.

V. INTERNAL REPORTING SYSTEM

40. The internal reporting system of the intermediary in micropayment shall contain at least the following elements:
- Data on risks identified with the risk analysis and conducted controls;

- Information on contracts with suppliers of products and services and micropayment users;
- Fulfillment of the performance and operational capacity indicators;
- Information on security incidents, fraud and reactions taken by the intermediary in micropayment;
- Identified needs for change in the information technology and information system security policy.

VI. TRANSITIONAL AND FINAL PROVISIONS

41. The intermediary in micropayment shall notify the National Bank of the changes in the technical standards of Sections II, III and IV in this Decision, eight days after the change.

42. This Decision shall enter into force within eight days from the date of its publication in the "Official Gazette of the Republic of Macedonia".

D.no.02-15/III-9-2013   **Dimitar Bogov**
March 28, 2013   **Governor**
Skopje

         Chairman
         of the National Bank of the Republic
         of Macedonia Council