Pursuant to Article 75d of the Law on Payment Services (RS Official Gazette, Nos 139/2014, 44/2018 and 64/2024) and Article 15, paragraph 1 and Article 63, paragraph 3 of the Law on the National Bank of Serbia (RS Official Gazette, Nos 72/2003, 55/2004, 85/200 – other law, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – CC Decision and 44/2018), the Executive Board of the National Bank of Serbia issues

DECISION ON TECHNICAL STANDARDS FOR STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

I. GENERAL PROVISIONS

1. This Decision establishes the requirements to be complied with by payment service providers for the purpose of establishing and implementing security measures when providing payment services, which enable them to do the following:

1) apply the procedure of strong authentication of payment service users (hereinafter: user);
2) apply exemptions from strong customer authentication;
3) protect the confidentiality and the integrity of the user's personalised security credentials;
4) establish common and secure open standards for the communication between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.

2. For the purposes of this Decision, the following definitions shall apply:

1) ***strong customer authentication*** means an authentication based on the use of two or more elements and/or a combination of these elements which must be independent, in that the breach of one does not compromise the reliability of the others, and designed in such a way as to protect the confidentiality of the authentication data. The elements used in such authentication shall belong to at least two of the following categories:
– knowledge (something only the user knows) – means the use of an element that only the user knows (e.g. password, personal identification number, answer to a specific question, swiping path, etc.),
– possession (something only the user possesses) – means the use

of an element that only the user possesses (e.g. a device or a telephone number which is registered and where evidence of possession is provided through the generation of a one-time password, a device where evidence of possession is provided through a digital signature or a standardised two-dimensional code – QR code, cryptographic key, application proved to be linked to a device, etc.),

– inherence (something only the user is) – means the use of elements typical only for the user (e.g. biometric characteristics, such as fingerprint, iris, voice, etc. or actions or behaviours recognised as belonging only to the user because of the way they are performed, such as signature, handwriting, keystroke dynamics, typing patterns, etc.);

2) ***electronic payment transaction*** means a payment transaction initiated and executed using an electronic platform or device, and does not include payment transactions initiated by means of a paper-based payment order;

3) ***interface*** means a logical component of the information-communication system through which, in accordance with a predefined set of routines and protocols, a communication channel is established and information is exchanged with other systems;

4) ***online connection*** means a connection between the provider and the user of a service through a publicly available communications network (e.g. the internet);

5) ***payment card*** means a payment instrument in the form of a physical or electronic card used to initiate a payment transaction, enabling its holder to make payments for goods and services either at an accepting device or by initiating the payment transaction remotely and/or to withdraw cash and/or use other services at an automated teller machine or another self-service device;

6) ***card-based payment instrument*** and payment application shall have the meaning laid down in the law regulating multilateral interchange fees and special operating rules for card-based payment transactions;

7) the terms ***authentication, personalised security credentials, sensitive payment data, remote payment transaction*** and ***credit transfer*** shall have the meanings laid down in the Law on Payment Services (hereinafter: Law);

8) **electronic communications network** shall have the meaning laid down in the law governing electronic communications.

II. STRONG CUSTOMER AUTHENTICATION

1. General authentication requirements

Transaction monitoring mechanisms

3. Payment service providers shall have effective transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent initiation of a payment transaction and/or abuse of such transaction, for the purpose of the implementation of the security measures referred to in Section 1, items 1) and 2) hereof.

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

Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:

1) lists of compromised or stolen authentication elements;
2) the amount of each payment transaction;
3) known fraud scenarios in the use and/or provision of payment services;
4) signs of malware infection in any sessions of the authentication procedure;
5) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the user and the abnormal use of the access device or the software.

Review of the security measures

4. The implementation of the security measures referred to in Section 1 hereof by the payment service provider shall be documented, periodically tested, evaluated and audited by auditors with expertise in information-communication system security and payment services that are operationally independent within (internal auditors) or from (external auditors) the payment service provider.

The audit referred to in paragraph 1 hereof shall be carried out at least once a year, and after major changes in the information-communication system.

Notwithstanding paragraph 1 hereof, where a payment service provider makes use of the exemption from strong authentication referred to in Section 20 hereof, the methodology, model and the reported misuses/frauds relating to such use shall be subject to an audit by an external auditor during the first year of making use of the exemption, and at least every three years during its use, or more frequently, at the request of the National Bank of Serbia.

The audit referred to in paragraph 1 hereof shall present an evaluation and report on the compliance of the payment service provider's security measures with the requirements set out in this Decision. The payment service provider shall make this report available to the National Bank of Serbia upon its request.

2. Security measures for the application of strong customer authentication

Authentication code

5. Where a payment service provider applies strong customer authentication, the authentication shall be based on two or more elements specified in Section 2, item 1) hereof and shall result in the generation of an authentication code.

The authentication code referred to in paragraph 1 hereof shall be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any other action through the internet and/or a device that can be used for remote communication, which may imply a risk of payment fraud or other abuses.

For the purpose of paragraphs 1 and 2 hereof, a payment service provider shall adopt security measures ensuring that each of the following requirements is met:

1) no information on any of the elements referred to in paragraph 1 hereof can be derived from the disclosure of the authentication code;
2) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;
3) the authentication code cannot be forged.

A payment service provider shall ensure that the authentication by means of generating an authentication code includes each of the following measures:

1) where the authentication for remote payment account access, initiation of remote electronic payments or any other actions through the internet and/or a device that can be used for remote communication, which may imply a risk of payment fraud or other abuses, has failed to generate an authentication code within the meaning of paragraph 1 hereof, it shall not be possible to identify which of the elements referred to in paragraph 1 hereof was incorrect;

2) the number of failed authentication attempts that can take place consecutively, after which the actions referred to in Article 75c of the Law shall be temporarily or permanently blocked, shall not exceed five;

3) the expiration time of the authentication code shall be limited to the time needed to perform authentication, and may not exceed 180 seconds;

4) the communication sessions are protected against the capture of or unauthorized access to the authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements of Chapter III hereof;

5) the maximum time without activity by the payer after being authenticated for accessing its payment account shall not exceed five minutes.

In case of the temporary block referred to in paragraph 4, item 2) hereof, the duration of that block and the number of retries shall be established 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 Section 3, paragraph 3 hereof.

A payment service provider shall alert the payer before the block referred to in paragraph 4, item 2) and paragraph 5 hereof is made permanent.

A payment service provider shall establish a secure procedure allowing the payer to regain use of the electronic payment instrument after the permanent block referred to in paragraph 6 hereof.

Dynamic linking

6. Where a payment service provider applies strong customer authentication to initiate a remote payment transaction, in addition to the requirements of Article 5 hereof, they shall also adopt security measures that meet the following requirements:

1) the payer is made aware of the amount of the payment transaction and of the payee;

2) 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;

3) 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;

4) any change to the amount or the payee results in the invalidation of the authentication code generated.

For the purpose of paragraph 1 hereof, a payment service provider shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:

1) the amount of the payment transaction and the payee throughout all of the phases of strong customer authentication;

2) the information displayed to the payer throughout all of the phases of strong customer authentication including the generation, transmission and use of the authentication code.

For the purpose of paragraph 1 hereof, the following requirements for the authentication code shall apply:

1) in relation to a card-based payment transaction for which the payer has given consent to the exact amount of the funds to be blocked pursuant to Article 49a, paragraph 1 of the Law, the authentication code shall be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction;

2) in relation to payment transactions for which the payer has given consent to execute a batch of remote 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 categorised as knowledge

7. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties.

The use by the payer of the elements referred to in paragraph 1 hereof shall be subject to mitigation measures applied by the payment service provider in order to prevent their disclosure to unauthorised parties.

Requirements of the elements categorised as possession

8. A payment service provider shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties.

The use by the payer of the elements referred to in paragraph 1 hereof shall be subject to mitigation measures applied by the payment service provider designed to prevent replication of the elements.

Requirements of devices and software linked to elements categorised as inherence

9. Payment service providers shall adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties.

At a minimum, the payment service provider shall ensure that the access devices and software referred to in paragraph 1 hereof have a very low probability of an unauthorised party being in the capacity of the payer instead of the payer and/or of being authenticated as the payer.

The use by the payer of the elements referred to in paragraph 1 hereof shall be subject to measures applied by the payment service provider ensuring that access devices and the software guarantee resistance against unauthorised use of the elements through access to these devices and the software.

Independence of the elements for strong customer authentication

10. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Sections 7 to 9 hereof is subject to measures which ensure that, in terms of technology, algorithms and parameters, 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 or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.

For the purpose of paragraph 2 hereof, the payment service provider shall set up the following mitigating measures:

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

3. Exemptions from strong customer authentication

Direct access to payment account information in the account servicing payment service provider

11. Account servicing payment service providers shall be allowed not to apply strong customer authentication where a user accesses the payment account online, subject to compliance in each case with the general authentication requirements referred to in Section 3 hereof, and where such access does not result in the disclosure of sensitive payment data and is limited to:

1) the balance of one or more designated payment accounts; or
2) payment transactions executed in the last 90 days through one or more designated payment accounts.

For the purpose of paragraph 1 hereof, payment service providers shall not be exempted from the application of strong customer authentication referred to in paragraph 1 hereof where either of the following conditions is met:

1) the user is accessing the information specified in that paragraph for the first time;
2) more than 180 days have elapsed since the last time the user accessed the information specified in that paragraph and strong customer authentication was applied.

Direct access to payment account information through an account information service provider

12. A payment service provider shall be allowed not to apply strong customer authentication where a user accesses the payment account online through an account information service provider, subject to compliance in each case with the general authentication requirements referred to in Section 3 hereof and where such access does not result in the disclosure of sensitive payment data and is limited to:

1) the balance of one or more designated payment accounts; or
2) payment transactions executed in the last 90 days through one or more designated payment accounts.

Notwithstanding paragraph 1 hereof, a payment service provider shall apply strong customer authentication referred to in that paragraph where either of the following conditions is met:

1) the user is accessing the information specified in that paragraph for

the first time;

2) more than 180 days have elapsed since the last time the user accessed the information specified in that paragraph and strong customer authentication was applied.

Notwithstanding paragraph 1 hereof, where a payment service provider has objectively justified and demonstrable reasons relating to unauthorised or fraudulent account access, the payment service provider may apply strong customer authentication when the user accesses the payment account online through an account information service provider. In that case, the payment service provider shall, upon the request of the National Bank of Serbia, document and justify the reasons for applying strong customer authentication.

An account servicing payment service provider which has established the dedicated interface referred to in Section 32 hereof shall not be required to apply the exemption referred to in paragraph 1 hereof for the contingencies referred to in Section 35, paragraph 5 hereof where such payment service provider does not apply the exemption referred to in Section 11 hereof through the direct interface used for authentication and communication with the users.

Contactless payments at point of sale

13. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general requirements laid down in Section 3 hereof, where the payer initiates a contactless electronic payment transaction provided that at least one of the following conditions are met:

1) the individual amount of the contactless electronic payment transaction does not exceed RSD 6,000, 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 RSD 18,000; or

2) 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

14. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general requirements laid down in Section 3 hereof, where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

Trusted beneficiaries

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

Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general requirements referred to in Section 3 hereof, where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries referred to in paragraph 1 hereof previously created by the payer.

Recurring transactions

16. Payment service providers shall apply strong customer authentication when a payer creates, amends, or initiates for the first time payment transactions recurring in given time intervals with the same amount and the same payee (a series of recurring transactions).

Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general requirements referred to in Section 3 hereof, for the initiation of all subsequent payment transactions included in the series of recurring payment transactions referred to in paragraph 1 hereof.

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

17. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements referred to in Section 3 hereof, where the payer initiates a credit transfer in circumstances where the payer and the payee are the same natural or legal person and both payment accounts are held by the same payment service provider.

Low-value transactions

18. Payment service providers shall be allowed not to apply strong customer authentication, where the payer initiates a remote electronic payment transaction provided that the following conditions are met:

1) the amount of the remote electronic payment transaction does not exceed RSD 3,600; and
2) the cumulative amount of previous remote electronic payment

transactions initiated by the payer since the last application of strong customer authentication does not exceed RSD 12,000; or

3) 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

19. A payment service provider shall be allowed not to apply strong customer authentication, in respect of legal persons and entrepreneurs initiating electronic payment transactions through the use of dedicated payment processes or protocols that are only made available to payers who are not consumers, if it has notified the National Bank of Serbia thereof at least 30 days before starting the provision of a payment service which includes such initiation of electronic payment transactions and submitted evidence that those processes or protocols guarantee at least equivalent levels of security to those provided for by the Law and this Decision.

Transaction risk analysis

20. Payment service providers shall be allowed not to apply 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 Section 3 hereof.

An electronic payment transaction referred to in paragraph 1 hereof shall be considered as posing a low level of risk where the following conditions are met:

1) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Section 21 hereof, is equivalent to or below the reference fraud rates specified in Annex 1, which is printed with this Decision and integral thereto;

2) the amount of the transaction does not exceed the relevant exemption threshold value specified in Annex 1;

3) payment service providers as a result of performing a real time risk analysis have not identified any of the following:

– abnormal spending or behavioural pattern of the payer;

– unusual information about the payer's device/software access;

– malware infection in any session of the consumer authentication procedure;

– known fraud scenario in the provision of payment services;

– abnormal location of the payer;

- high-risk location of the payee.

Payment service providers that intend to exempt electronic remote payment transactions referred to in paragraph 1 hereof from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

1) the previous spending patterns of the individual user to whose transactions the exemption would apply;
2) the payment transaction history of each of the payment service provider's payment service users;
3) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;
4) the identification of abnormal payment patterns of the specific user in relation to whose transactions the exemption would apply, taking into account the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors referred to in paragraph 3 hereof into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

Calculation of fraud rates

21. The payment service provider shall ensure that the overall fraud rates for card-based remote electronic transactions and remote electronic credit transfers, including payment transactions authenticated through strong customer authentication and those executed under any of the exemptions referred to in Sections 15 to 20 hereof, are equivalent to, or lower than, the reference fraud rate for the same type of transaction indicated in Annex 1.

The overall fraud rate for each type of transaction referred to in paragraph 1 hereof shall be calculated as the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under any exemption referred to in Sections 15 to 20 hereof on a rolling quarterly basis (90 days).

The payment service provider shall document the methodology and the model used to calculate the fraud rates referred to in paragraph 1 hereof, as well as the fraud rates themselves, and make them available to the National Bank of Serbia upon request.

Cessation of exemptions based on transaction risk analysis

22. Payment service providers that do not apply strong customer authentication in line with Section 20 hereof shall immediately report to the National Bank of Serbia where one of their monitored fraud rates, for any type of payment transactions set out in Annex 1, exceeds the applicable reference fraud rate and shall at the same time 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.

The payment service providers referred to in paragraph 1 hereof shall immediately start applying strong customer authentication for any type of payment transactions indicated in the Annex 1 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.

In the event referred to in paragraph 2 hereof, payment service providers shall apply strong customer authentication until their calculated fraud rate equals to, or is below, the reference fraud rates applicable for that type of payment transaction in that exemption threshold range for one quarter.

Where payment service providers intend to cease to apply strong customer authentication again in accordance with Section 20 hereof, they shall notify the National Bank of Serbia thereof at least 30 days before the intended cessation and provide evidence of the restoration of compliance of their monitored fraud rate with the applicable reference fraud rate for that exemption threshold range in accordance with paragraph 3 of this Section.

Monitoring payment transactions

23. Payment service providers not applying strong customer authentication in accordance with Sections 11 to 20 hereof shall record and monitor the following data for each type of payment transactions, with a breakdown for both remote and non-remote payment transactions, at least on a quarterly basis:

1) the total value of unauthorised or fraudulent payment transactions in accordance with the provisions of the Law regulating the conditions and manner of executing payment transactions, as well as 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 in accordance with the provisions hereof;

2) the average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under each

of the exemptions in accordance with the provisions hereof;

3) the number of payment transactions where each of the exemptions was applied and their percentage in respect of the total number of payment transactions, for each of the exemptions in accordance with the provisions hereof.

Payment service providers shall make the results of the monitoring in accordance with paragraph 1 hereof available to the National bank of Serbia upon its request.

4. Confidentiality and integrity of users' personalised security credentials

General requirements for confidentiality and integrity of personalised security credentials

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

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

1) personalised security credentials are masked when displayed and are not readable in their full extent when input by the user during the authentication;

2) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plain text;

3) secret cryptographic material is protected from unauthorised disclosure.

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

Payment service providers shall ensure that the processing and routing of personalised security credentials and the authentication codes generated in accordance with Sections 5 to 10 hereof – take place in secure environments in accordance with the regulations governing this area and reliable and widely recognised industry standards.

Creation and transmission of personalised security credentials

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

Payment service providers shall apply measures to mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software following their loss, theft or copying before their delivery to the payer of those personalised security credentials and the authentication devices and software.

Association with the user

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

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

1) the association of the user's identity with personalised security credentials, authentication devices and software is carried out in secure environments under the payment service provider’s responsibility comprising at least the payment service provider’s premises, the internet environment provided by the payment service provider or secure websites used by the payment service provider and its automated teller machine services, and taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the payment service provider;

2) the association by means of a remote channel of the user’s identity with the personalised security credentials and with authentication devices or software is performed using strong customer authentication.

Delivery of personalized security credentials, authentication devices and software

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

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

1) effective and secure delivery mechanisms ensuring that the personalised security credentials, authentication devices and software are delivered to the legitimate user;

2) mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the user by means of the internet;

3) arrangements ensuring that, where the delivery of personalised security credentials is executed outside the premises of the payment service provider or through a remote channel:

– no unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software when delivered through the same channel,

– the delivered personalised security credentials, authentication devices or software require activation before usage;

4) arrangements ensuring that, in cases where the personalised 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 Section 26 hereof.

Renewal and re-activation of personalised security credentials

28. Payment service providers shall ensure that the renewal or re-activation of personalised security credentials adhere to the procedures for the creation, association and delivery of the credentials and of the authentication devices in accordance with Sections 25 to 27 of this Decision.

Destruction, deactivation and revocation

29. Payment service providers shall ensure that they have effective processes in place to apply each of the following security measures:

1) the secure destruction, deactivation or revocation of the personalised security credentials, authentication devices and software;

2) where the payment service provider distributes reusable authentication devices and software – the secure re-use of a device or software is established, documented and implemented before making it available to another user;

3) the deactivation or revocation of information related to personalised security credentials stored in the payment service provider's systems and databases and, where relevant, in public repositories.

III. COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

1. General requirements for communication

Requirements for identification

30. Payment service providers shall ensure secure identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals.

Payment service providers shall apply measures to ensure that the risks of misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.

Traceability

31. Payment service providers shall have processes in place which ensure that all payment transactions and other interactions with the user, with other payment service providers and with other entities, including merchants, in the context of the provision of the payment service are traceable, ensuring knowledge ex post of all events relevant to the electronic transaction in all the various stages.

For the purpose of paragraph 1 hereof, payment service providers shall ensure that any communication session established with the user, other payment service providers and other entities, including merchants, relies on each of the following:

1) a unique identifier of the communication session;
2) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data;
3) timestamps of the communication session.

The timestamps referred to in paragraph 2, items 2) and 3) hereof must be based on a unified time-reference system and synchronised according to the official time signal in the Republic of Serbia.

2. Specific requirements for the common and secure open standards of communication

General obligations for access interfaces

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

1) 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 based on the payment card;

2) 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;

3) payment initiation service providers are able to communicate securely to initiate a payment order from the payer’s payment account and receive all information on the initiation of the payment transaction and all information accessible to the account servicing payment service providers regarding the execution of the payment transaction.

For the purpose of authentication of the user, the interface referred to in paragraph 1 hereof shall allow account information service providers and payment initiation service providers to rely on all the authentication procedures provided by the account servicing payment service provider to the user.

The interface referred to paragraph 1 hereof shall at least meet all of the following requirements:

1) 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 based on the consent of the user;

2) communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and any user concerned shall be established and maintained throughout the authentication;

3) the integrity and confidentiality of the personalised security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider shall be ensured.

All communication between account information service providers and payment initiation service providers and account servicing payment service providers shall take place through dedicated interfaces developed by the National Bank of Serbia.

Account servicing payment service providers shall make available a testing facility, including support, for connection and functional testing to enable authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or entities that have applied with the National Bank of Serbia for the relevant authorization to provide any of these payment services, to test their software and applications used for offering a payment service to users.

The testing facility referred to in paragraph 5 hereof should enable the interface testing in the manner set out in Section 5, paragraph 5 of Annex 2 printed herewith and integral hereto, and should be made available before the target date for the market launch of the access interface referred to in paragraph 1 hereof.

The testing facility referred to in paragraph 5 hereof shall not be used for sharing sensitive information, especially sensitive payment data.

In the event that the interface referred to in paragraph 1 hereof is not in compliance with the requirements set out in this Decision, account servicing payment service providers shall ensure that the provision of payment initiation services and account information services is not prevented or disrupted at any moment to the extent that the respective providers of such services comply with the conditions defined under Section 35, paragraphs 6 and 7 of this Decision.

In relation to the dedicated interface referred to in paragraph 4 hereof, the National Bank of Serbia shall ensure the testing facility by applying mutatis mutandis the provisions of paragraphs 5 to 7 hereof.

Access interface options

33. Account servicing payment service providers shall establish the interface(s) referred to in Section 32 hereof by means of a dedicated interface, by enabling the use of the dedicated interface referred to in Section 32, paragraph 4 hereof or by allowing the use by the payment service providers referred to in Section 32, paragraph 1 hereof of the interfaces used for authentication and communication with the account servicing payment service provider’s users.

Obligations for a dedicated interface

34. Subject to compliance with Sections 32 and 33 hereof, account servicing payment service providers that have put in place a dedicated interface shall ensure that the dedicated interface offers at all times the same level of availability and performance, including support, as the interfaces made available to the user for directly accessing its payment account online.

Account servicing payment service providers that have put in place a dedicated interface shall define transparent key performance indicators and service level targets, at least as stringent as those set for the interface used by their payment service users both in terms of availability and of data provided in accordance with Section 38 hereof.

The payment service provider shall perform stress-testing of the provision of services through the dedicated interface referred to in paragraph

2 hereof.

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.

The obstacles referred to in paragraph 4 hereof include, in particular, preventing the use by payment service providers referred to in Section 32, paragraph 1 hereof of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing payment service provider's authentication or other functions, requiring additional authorisations and registrations in addition to those provided for by Law, or requiring additional checks of the consent given by users to providers of payment initiation and account information services.

The National Bank of Serbia shall establish dedicated interfaces from Section 32, paragraph 4 hereof in accordance with the requirements set out in this Section and in such a manner as to enable the payment service providers from Section 32, paragraph 1 hereof to meet their obligations defined herein.

The National Bank of Serbia shall monitor the availability and performance of the dedicated interface referred to in Section 32, paragraph 4 hereof and shall publish on its website quarterly statistics on the availability and performance of the dedicated interfaces.

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

Contingency measures for a dedicated interface

35. The establishment of a dedicated interface referred to in Section 32, paragraph 4 hereof shall include a strategy and plans for contingency measures for the event that the interface does not perform in compliance with Section 34 hereof, that there is unplanned unavailability of the interface and that there is a system breakdown.

Unplanned unavailability or a system breakdown within the meaning of paragraph 1 hereof 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.

The contingency measures referred to in paragraph 1 hereof shall include communication plans to inform payment service providers making use of the dedicated interface of measures to restore the system and a description of the immediately available alternative options payment service providers may have during this time.

Both the account servicing payment service provider and the payment service providers referred to in Section 32, paragraph 1 hereof shall report problems with dedicated interfaces as described in paragraphs 1 and 2 hereof to the National Bank of Serbia without delay.

Account servicing payment service providers shall establish a contingency mechanism enabling payment service providers referred to in Section 32, paragraph 1 hereof to make use of the interfaces made available to their payment service users for the authentication and communication with their account servicing payment service provider, until the dedicated interface is restored to the level of availability and performance provided for in Article 33 hereof.

For the purpose of paragraph 5 hereof, account servicing payment service providers shall ensure that the payment service providers referred to in Section 32, paragraph 1 hereof can be identified and can rely on the authentication procedures provided by the account servicing payment service provider to the user.

Where the payment service providers referred to in Section 32, paragraph 1 hereof make use of the interface referred to in paragraph 5 hereof they shall:

1) take the necessary measures to ensure that they do not access, store or process data for purposes other than for the provision of the service as requested by the user;
2) continue to comply with the obligations following from Article 46b, paragraph 2 and Article 46c, paragraph 2 of the Law;
3) log the data that are accessed through the interface operated by the account servicing payment service provider for its payment service users, and provide, upon request and without undue delay, the log files to the National Bank of Serbia;
4) duly justify to the National Bank of Serbia, upon request and without undue delay, the use of the interface made available to the users for directly accessing their payment accounts online;
5) inform the account servicing payment service provider accordingly.

The National Bank of Serbia may exempt the account servicing payment service providers that have opted for a dedicated interface from the obligation to set up the contingency mechanism described under paragraph 5 hereof if based on the information and data provided by that payment service provider in relation to the interface made available to its payment service users for user authentication and communication meets the following conditions:

1) the access interface made available by that payment service provider complies with the same obligations in terms of the level of availability and performance, including support and additional obligations set out in Annex 2 hereof;
2) the access interface has been designed and tested in accordance with Section 32, paragraphs 5 to 7 hereof to the satisfaction of the payment service providers referred to Section 32, paragraph 5 hereof;
3) it has been widely used for at least 3 months by payment service providers to offer account information services, payment initiation services and to provide confirmation on the availability of funds for card-based payments.

If the payment service providers referred to in paragraph 8 hereof do not meet the obligations from provisions under 1) and 4) hereof – they shall set up a contingency mechanism referred to in paragraph 5 hereof at the latest within two months from the establishment of the failure to meet those obligations.

Certificates

36. For the purpose of identification, as referred to in Section 32, paragraph 1, item 1) hereof, payment service providers shall rely on qualified certificates for electronic seals or qualified certificates for website authentication within the meaning of the law governing electronic documents, electronic identification and trust services in electronic business which will be issued by the National Bank of Serbia.

The certificate referred to in paragraph 1 hereof shall include, in Serbian or in English, each of the following:

1) the role of the payment service provider, namely:
   - account servicing,
   - payment initiation,
   - account information, and/or
   - issuing of card-based payment instruments;

2) the name “National Bank of Serbia” as the competent authority that issued the license to provide payment services to the payment service provider.

The data referred to in paragraph 2 hereof shall not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

Security of communication session

37. 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 exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments 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.

When maintaining parallel network sessions with the account servicing payment service provider, account information service providers and payment initiation service providers shall ensure that those sessions are securely linked to relevant sessions established with the user(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.

To prevent the possibility of misrouting messages or information that are communicated, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall contain unambiguous references with the account servicing payment service provider to each of the following items:

1) the user or users and the corresponding communication session in order to distinguish several requests from the same user or users;
2) for payment initiation services – the uniquely identified payment transaction initiated;
3) 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.

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 where they communicate personalised security credentials and authentication codes, these are not readable at any time, directly or indirectly, by any staff or other persons engaged by those payment service providers.

In case of loss of confidentiality of personalised security credentials under their sphere of competence, the payment service providers referred to in paragraph 5 hereof shall inform without undue delay the user associated with them and the issuer of the personalised security credentials.

Data exchanges

38. Account servicing payment service providers shall comply with each of the following requirements:

1) they shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the user when directly requesting access to the account information, provided that this information does not include sensitive payment data;
2) 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 user when the transaction is initiated directly by the latter;
3) 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.

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.

Where the account servicing payment service provider offers a dedicated interface in accordance with Section 34 hereof, the interface shall provide for notification messages concerning unexpected events or errors to be communicated by any payment service provider that detects the event or error to the other payment service providers participating in the communication session.

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

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

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:

1) whenever the user is actively requesting such information;
2) where the 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 user's consent.

IV. TRANSITIONAL AND FINAL PROVISIONS

39. Payment service providers shall harmonise their internal acts with the provisions of this Decision by no later than a month before the start of its application and shall submit to the National Bank of Serbia within that deadline a notification thereon and the relevant harmonised internal acts.

40. This Decision shall not apply to a bank merging with another bank, if the acquiring bank filed to the National Bank of Serbia a duly completed application for consent to the merger by acquisition at the latest by the start of application of this Decision and the planned date of registration of status change is no later than 31 December 2026.

A bank which submitted to the National Bank of Serbia before the start of application of this Decision the notification and the decision of the bank’s managing body on the planned data migration to a new core business application within the meaning of the decision governing minimum standards of information-communication system management for financial institutions shall be subject to the provisions of this Decision as of 30 June 2026.

41. This Decision shall enter into force on the eighth day following its publication in the RS Official Gazette and shall apply as of 1 January 2026.

NBS EB No 84
20 December 2024
Belgrade

Chairperson
NBS Executive Board
Governor
National Bank of Serbia

Dr Jorgovanka Tabaković