Pursuant to Article 35, paragraph 1 subparagraph 1.1 and Article 65 of the Law No. 03/L-209 on Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No.77 / 16 August 2010), amended and supplemented by Law No. 05/L –150 (Official Gazette of the Republic of Kosovo / No. 10 / 03 April 2017) and pursuant to Article 98 and 135 of the Law No. 08/L-328 on Payment Services, the Board of the Central Bank of the Republic of Kosovo, at its meeting held on December 17, 2024, approved the following:

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

CHAPTER I

GENERAL PROVISIONS

Article 1
Purpose and Scope

1. The purpose of this Regulation is to establish the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to do the following:
   1.1. apply the procedure of strong customer authentication in accordance with Article 97 of Law No. 08/L-328 on Payment Services;
   1.2. exempt the application of the security requirements of strong customer authentication, subject to specified and limited conditions based on the level of risk, the amount and the recurrence of the payment transaction and of the payment channel used for its execution;
   1.3. protect the confidentiality and the integrity of the PSU's personalized security credentials;
   1.4. 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 in relation to the provision and use of payment services in application of Section IV of the Law No. 08/L-328 on Payment Services.
2. This regulation shall apply to payment service providers, as defined in article 1, paragraph 1 of Law No. 08/L-328 on Payment Services.

Article 2
Definitions

1. The terms and definitions used in this Regulation shall have the same meaning as in the Law No. 08/L-328 on Payment Services.
2. In addition to paragraph 2, for the purpose of implementing this Regulation, the following terms and abbreviations shall have the following meanings:

   2.1. **"ASPSP"** means an account servicing payment service provider;

   2.2. **"AIS"** means account information services;

   2.3. **"AISP"** means account information service provider;

   2.4. **"CBK"** means the Central Bank of the Republic of Kosovo;

   2.5. **"EBA"** means the European Banking Authority;

   2.6. **"ETV"** means exemption threshold value;

   2.7. **"Law on Payment Services"** means Law No. 08/L-328 on Payment Services;

   2.8. **"PIS"** means payment initiation services;

   2.9. **"PISP"** means payment initiation service provider;

   2.10. **"PSP"** means payment service provider;

   2.11. **"PSU"** means payment service user.

Article 3
General authentication requirements

1. PSPs 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 subparagraphs 1.1 and 1.2 of Article 1.

   1.1. those mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the PSU in the circumstances of a normal use of the personalized security credentials.

2. PSPs shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:

   2.1. lists of compromised or stolen authentication elements;

   2.2. the amount of each payment transaction;

   2.3. known fraud scenarios in the provision of payment services;

   2.4. signs of malware infection in any sessions of the authentication procedure;

   2.5. in case the access device or the software is provided by the PSP, a log of the use of the access device or the software provided to the PSU and the abnormal use of the access device or the software.

Article 4
Review of the security measures

1. The implementation of the security measures referred to in Article 1 of this regulation shall be documented, periodically tested, evaluated and audited in accordance with the applicable legal framework of the PSP by auditors with expertise in ICT (Information technology and communication) security and payments and operationally independent within or from the PSP.
2. The period between the audits referred to in paragraph 1 shall of this article be determined taking into account the relevant accounting and statutory audit framework applicable to the PSP.
   2.1. however, PSPs that make use of the exemption referred to in Article 18 of this regulation shall be subject to an audit of the methodology, the model and the reported fraud rates at a minimum on a yearly basis. The auditor performing this audit shall have expertise in ICT security and payments and be operationally independent within or from the PSP. During the first year of making use of the exemption under Article 18 of this regulation and at least every 3 years thereafter, or more frequently at the CBK's request, this audit shall be carried out by an independent and qualified external auditor.
3. This audit shall present an evaluation and report on the compliance of the PSP's security measures with the requirements set out in this Regulation. Report shall be made available to the CBK upon request.

CHAPTER II

SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

Article 5
Authentication code

1. Where PSPs apply strong customer authentication in accordance with Article 97 paragraph 1 of the Law on Payment Services, the authentication shall be based on two or more elements which are categorized as knowledge, possession and inherence and shall result in the generation of an authentication code.
   1.1. the authentication code shall be only accepted once by the PSP when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.
2. For the purpose of paragraph 1 of this article, PSPs shall adopt security measures ensuring that each of the following requirements is met:
   2.1. no information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code;
   2.2. it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;
   2.3. the authentication code cannot be forged.
3. PSPs shall ensure that the authentication by means of generating an authentication code includes each of the following measures:

3.1. where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1 of this article, it shall not be possible to identify which of the elements referred to in that paragraph was incorrect;

3.2. the number of failed authentications attempts that can take place consecutively, after which the actions referred to in Article 97 paragraph 1 of the Law on Payment Services shall be temporarily or permanently blocked, shall not exceed five within a given period of time;

3.3. the communication sessions are 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 of this regulation;

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

4. Where the block referred to in subparagraph 3.2 of this article is temporary, 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 Article 3 paragraph 2 of this regulation.

4.1. the payer shall be alerted before the block is made permanent;

4.2. where the block has been made permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments.

Article 6
Dynamic linking

1. Where PSPs apply strong customer authentication in accordance with Article 97 paragraph 2 of the Law on Payment Services, in addition to the requirements of Article 5 of this Regulation, they shall also adopt security measures that meet each of the following requirements:

1.1. the payer is made aware of the amount of the payment transaction and of the payee;

1.2. 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;

1.3. the authentication code accepted by the PSP corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;

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

2. For the purpose of paragraph 1 of this article, PSPs shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:

2.1. the amount of the transaction and the payee throughout all of the phases of the authentication;

2.2. the information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code.

3. For the purpose of subparagraph 1.2 and where PSPs apply strong customer authentication in accordance with Article 97 paragraph 2 of the Law on Payment Services the following requirements for the authentication code shall apply:

   3.1. 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 75 paragraph 1 of the Law on Payment Services, 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;

   3.2. 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.

Article 7
Requirements of the elements categorized as knowledge

1. PSPs shall adopt measures to mitigate the risk that the elements of strong customer authentication categorized as knowledge are uncovered by, or disclosed to, unauthorized parties.
2. The use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorized parties.

Article 8
Requirements of the elements categorized as possession

1. PSPs shall adopt measures to mitigate the risk that the elements of strong customer authentication categorized as possession are used by unauthorized parties.
2. The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.

Article 9
Requirements of devices and software linked to elements categorized as inherence

1. PSPs shall adopt measures to mitigate the risk that the authentication elements categorized as inherence and read by access devices and software provided to the payer are uncovered by unauthorized parties. At a minimum, the PSPs shall ensure that those access devices and software have a very low probability of an unauthorized party being authenticated as the payer.
2. The use by the payer of those elements 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.

Article 10
Independence of the elements

1. PSPs shall ensure that the use of the elements of strong customer authentication referred to in Articles 7, 8 and 9 of this regulation, 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.
2. PSPs 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.
3. For the purposes of paragraph 2 of this article, the mitigating measures shall include each of the following:
   3.1. the use of separated secure execution environments through the software installed inside the multi-purpose device;
   3.2. mechanisms to ensure that the software or device has not been altered by the payer or by a third party;
   3.3. where alterations have taken place, mechanisms to mitigate the consequences thereof.

CHAPTER III

EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

Article 11

Access to the payment account information directly with the account servicing payment service provider or through an account information service provider

1. PSPs shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 3 of this regulation, where a PSU is accessing its payment account online directly, provided that access is limited to one of the following items online without disclosure of sensitive payment data:
   1.1. the balance of one or more designated payment accounts;
   1.2. the payment transactions executed in the last 90 days through one or more designated payment accounts.
2. By way of derogation from paragraph 1, PSPs shall not be exempted from the application of strong customer authentication where one of the following conditions is met:
   2.1. the PSU is accessing online the information specified in paragraph 1 for the first time;
   2.2. more than 180 days have elapsed since the last time the PSU accessed online the information specified in paragraph 1 of this article and strong customer authentication was applied.
3. PSPs shall not apply strong customer authentication where a PSU is accessing its payment account online through an AISP, provided that access is limited to one of the following items online without disclosure of sensitive payment data:
   3.1. the balance of one or more designated payment accounts;
   3.2. the payment transactions executed in the last 90 days through one or more designated payment accounts.

4. By way of derogation from paragraph 3, PSPs shall apply strong customer authentication where one of the following conditions is met:

   4.1. the PSU is accessing online the information specified in paragraph 3 of this article for the first time through the AISP;

   4.2. more than 180 days have elapsed since the last time the PSU accessed online the information specified in paragraph 3 of this article through the AISP and strong customer authentication was applied.

5. By way of derogation from paragraph 3 of this article, PSPs shall be allowed to apply strong customer authentication where a PSU is accessing its payment account online through an AISP and the PSP has objectively justified and duly evidenced reasons relating to unauthorized or fraudulent access to the payment account. In such a case, the PSP shall document and duly justify to the CBK, upon request, the reasons for applying strong customer authentication.

6. ASPSPs that offer a dedicated interface as referred to in Article 32 shall not be required to implement the exemption laid down in paragraph 3 of this Article for the purpose of the contingency mechanism referred to in Article 34 paragraph 4, where they do not apply the exemption laid down in paragraphs 1 and 2 of this Article in the direct interface used for authentication and communication with their PSUs.

Article 12
Contactless payments at point of sale

1. PSPs shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 of this regulation, where the payer initiates a contactless electronic payment transaction provided that the following conditions are met:

   1.1. the individual amount of the contactless electronic payment transaction does not exceed EUR 50; and

   1.2. 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 EUR 150; or

   1.3. 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 transactions.

Article 13
Unattended terminals for transport fares and parking fees

PSPs shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 3 of this regulation, 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.

Article 14

Trusted beneficiaries

1. PSPs shall apply strong customer authentication where a payer creates or amends a list of trusted beneficiaries through the payer's ASPSP.
2. PSPs shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

Article 15
Recurring transactions

1. PSPs shall apply strong customer authentication when a payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee.
2. PSPs shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred to in paragraph 1 of this article.

Article 16
Credit transfers between accounts held by the same natural or legal person

PSPs shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 3 of this regulation, 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 ASPSP.

Article 17
Low-value transactions

1. PSPs 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:
    1.1. the amount of the remote electronic payment transaction does not exceed EUR 30; and
    1.2. the cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed EUR 100; or
    1.3. 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.

Article 18
Secure corporate payment processes and protocols

PSPs shall be allowed not to apply 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 the CBK is satisfied that those processes

or protocols guarantee at least equivalent levels of security to those provided for by the Law on Payment Services.

Article 19
Transaction risk analysis

1. PSPs shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the PSP as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 3 and in subparagraph 2.3 of this Article.
2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:
   2.1. the fraud rate for that type of transaction, reported by the PSP and calculated in accordance with Article 20 of this regulation, is equivalent to or below the reference fraud rates specified in the table set out in the Annex 1 of this regulation for "remote electronic card-based payments" and "remote electronic credit transfers" respectively;
   2.2. the amount of the transaction does not exceed the relevant ETV specified in the table set out in the Annex 1 of this regulation;
   2.3. PSPs as a result of performing a real time risk analysis have not identified any of the following:
      2.3.1. abnormal spending or behavioral pattern of the payer;
      2.3.2. unusual information about the payer's device/software access;
      2.3.3. malware infection in any session of the authentication procedure;
      2.3.4. known fraud scenario in the provision of payment services;
      2.3.5. abnormal location of the payer;
      2.3.6. high-risk location of the payee.
3. PSPs that intend to exempt electronic remote payment transactions 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:
   3.1. the previous spending patterns of the individual PSU;
   3.2. the payment transaction history of each of the PSP's PSUs;
   3.3. 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 PSP;
   3.4. the identification of abnormal payment patterns of the PSU in relation to the user's payment transaction history.
4. The assessment made by a PSP under the previous paragraph shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

Article 20
Calculation of fraud rates

1. For each type of transaction referred to in the table set out in the Annex 1 of this regulation, the PSP shall 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 Articles 14 to 19 of this regulation are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction indicated in the table set out in the Annex of this regulation.

    1.1. the overall fraud rate for each type of transaction 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 transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under any exemption referred to in Articles 14 to 19 of this regulation on a rolling quarterly basis (90 days).

2. The calculation of the fraud rates and resulting figures shall be assessed by the audit review referred to in Article 4 paragraph 2 of this regulation, which shall ensure that they are complete and accurate.

3. The methodology and any model, used by the PSP to calculate the fraud rates, as well as the fraud rates themselves, shall be adequately documented and made fully available to the CBK.

Article 21
Cessation of exemptions based on transaction risk analysis

1. PSPs that make use of the exemption referred to in Article 18 of this regulation shall immediately report to the CBK where one of their monitored fraud rates, for any type of payment transactions indicated in the table set out in the Annex 1 of this regulation, exceeds the applicable reference fraud rate and shall provide to the CBK a description of the measures that they intend to adopt to restore compliance of their monitored fraud rate with the applicable reference fraud rates.

2. PSPs shall immediately cease to make use of the exemption referred to in Article 19 of this regulation for any type of payment transactions indicated in the table set out in the Annex 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.

3. Following the cessation of the exemption referred to in Article 19 of this regulation in accordance with paragraph 2 of this Article, PSPs 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 in that exemption threshold range for one quarter.

4. Where PSPs intend to make use again of the exemption referred to in Article 19 of this regulation, they shall notify the CBK in a reasonable timeframe and shall before making use again of the exemption, 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 Article.

Article 22
Monitoring

1. In order to make use of the exemptions set out in Articles 11 to 19 of this regulation, PSPs 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:
   1.1. the total value of unauthorized or fraudulent payment transactions in accordance with Article 64 paragraph 2 of the Law on Payment Services, 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;
   1.2. the average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions;
   1.3. the number of payment transactions where each of the exemptions was applied and their percentage in respect of the total number of payment transactions.
2. PSPs shall make the results of the monitoring in accordance with paragraph 1 of this article available to the CBK.

CHAPTER IV

CONFIDENTIALITY AND INTEGRITY OF THE PAYMENT SERVICE USERS' PERSONALISED SECURITY CREDENTIALS

Article 23
General requirements

1. PSPs shall ensure the confidentiality and integrity of the personalized security credentials of the PSU, including authentication codes, during all phases of the authentication.
2. For the purpose of paragraph 1 of this article, PSPs shall ensure that each of the following requirements is met:
   2.1. personalized security credentials are masked when displayed and are not readable in their full extent when input by the PSU during the authentication;
   2.2. personalized security credentials in data format, as well as cryptographic materials related to the encryption of the personalized security credentials are not stored in plain text;
   2.3. secret cryptographic material is protected from unauthorized disclosure.
3. PSPs shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalized security credentials.
4. PSPs shall ensure that the processing and routing of personalized security credentials and of the authentication codes generated in accordance with Chapter II of this regulation take place in secure environments in accordance with strong and widely recognized industry standards.

Article 24
Creation and transmission of credentials

1. PSPs shall ensure that the creation of personalized security credentials is performed in a secure environment.

   1.1. they 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.

Article 25
Association with the payment service user

1. PSPs shall ensure that only the PSU is associated, in a secure manner, with the personalized security credentials, the authentication devices and the software.
2. For the purpose of paragraph 1, PSPs shall ensure that each of the following requirements is met:

   2.1. the association of the PSU's identity with personalized security credentials, authentication devices and software is carried out in secure environments under the PSP's responsibility comprising at least the PSP's premises, the internet environment provided by the PSP or other similar secure websites used by the PSP 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 PSP;

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

Article 26
Delivery of credentials, authentication devices and software

1. PSPs shall ensure that the delivery of personalized security credentials, authentication devices and software to the PSU is carried out in a secure manner designed to address the risks related to their unauthorized use due to their loss, theft or copying.
2. For the purpose of paragraph 1, PSPs shall at least apply each of the following measures:

   2.1. effective and secure delivery mechanisms ensuring that the personalized security credentials, authentication devices and software are delivered to the legitimate PSU;

   2.2. mechanisms that allow the PSP to verify the authenticity of the authentication software delivered to the PSU by means of the internet;

   2.3. arrangements ensuring that, where the delivery of personalized security credentials is executed outside the premises of the PSP or through a remote channel:

      2.3.1. 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;

      2.3.2. the delivered personalized security credentials, authentication devices or software require activation before usage;

2.4. 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 Article 25 of this regulation.

Article 27
Renewal of personalized security credentials

PSPs shall ensure that the renewal or re-activation of personalized security credentials adhere to the procedures for the creation, association and delivery of the credentials and of the authentication devices in accordance with Articles 24, 25and 26.

Article 28
Destruction, deactivation and revocation

1. PSPs shall ensure that they have effective processes in place to apply each of the following security measures:
   1.1. the secure destruction, deactivation or revocation of the personalized security credentials, authentication devices and software;
   1.2. where the PSP 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 PSU;
   1.3. the deactivation or revocation of information related to personalized security credentials stored in the PSP's systems and databases and, where relevant, in public repositories.

CHAPTER V
COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

Subchapter I
General requirements for communication

Article 29
Requirements for identification

1. PSPs 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.
2. PSPs shall ensure that the risks of misdirection of communication to unauthorized parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.

Article 30
Traceability

1. PSPs shall have processes in place which ensure that all payment transactions and other interactions with the PSU, with other PSPs 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.
2. For the purpose of paragraph 1, PSPs shall ensure that any communication session established with the PSU, other PSPs and other entities, including merchants, relies on each of the following:
   2.1. a unique identifier of the session;
   2.2. security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data;
   2.3. timestamps which shall be based on a unified time-reference system and which shall be synchronized according to an official time signal.

Subchapter II
Specific requirements for the common and secure open standards of communication

Article 31
General obligations for access interfaces

1. ASPSPs 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:
   1.1. AISPs, PISPs and PSPs issuing card-based payment instruments are able to identify themselves towards the ASPSP;
   1.2. AISPs are able to communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions;
   1.3. PISPs 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 ASPSP regarding the execution of the payment transaction.
2. For the purposes of authentication of the PSU, the interface referred to in paragraph 1 of this article, shall allow AISPs and PISPs to rely on all the authentication procedures provided by the ASPSP to the PSU.
3. The interface referred to in paragraph 1 of this article, shall at least meet all of the following requirements:
   3.1. a PISP or an AISP shall be able to instruct the ASPSP to start the authentication based on the consent of the PSU;
   3.2. communication sessions between the ASPSP, the AISP, the PISP and any PSU concerned shall be established and maintained throughout the authentication;
   3.3. the integrity and confidentiality of the personalized security credentials and of authentication codes transmitted by or through the PISP or the AISP shall be ensured.

4. ASPSPs shall ensure that their interfaces follow standards of communication which are issued by international standardization organizations.

   4.1. ASPSPs shall also ensure that the technical specification of any of the interfaces is documented specifying a set of routines, protocols, and tools needed by PISPs, AISPs and PSPs issuing card-based payment instruments for allowing their software and applications to interoperate with the systems of the ASPSP;

   4.2. ASPSPs shall at a minimum, and no less than 6 months before the end of the transitional period referred to in Article 40, or before the target date for the market launch of the access interface when the launch takes place after the date referred to in Article 40, make the documentation available, at no charge, upon request by authorized PISPs, AISPs and PSPs issuing card-based payment instruments or PSPs that have applied to the CBK for the relevant authorization, and shall make a summary of the documentation publicly available on their website.

5. In addition to paragraph 4, ASPSPs shall ensure that, except for emergency situations, any change to the technical specification of their interface is made available to authorized PISPs, AISPs and PSPs issuing card-based payment instruments, or PSPs that have applied to the CBK for the relevant authorization, in advance as soon as possible and not less than 3 months before the change is implemented.

   5.1. PSPs shall document emergency situations where changes were implemented and make the documentation available to the CBK on request.

6. By way of derogation from paragraph 5 of this article, ASPSPs shall make available to the PSPs referred to in this Article the changes made to the technical specifications of their interfaces in order to comply with Article 11 paragraphs 3 to 6, not less than 2 months before such changes are implemented.

7. ASPSPs shall make available a testing facility, including support, for connection and functional testing to enable authorized PISPs, PSPs issuing card-based payment instruments and AISPs, or PSPs that have applied for the relevant authorization, to test their software and applications used for offering a payment service to users. This testing facility should be made available no later than 6 months before the application date referred to in Article 40 or before the target date for the market launch of the access interface when the launch takes place after the date referred to in Article 40.

   7.1. however, no sensitive information shall be shared through the testing facility.

8. The CBK shall ensure that ASPSPs comply at all times with the obligations included in this Regulation in relation to the interface(s) that they put in place. In the event that an ASPSP provider fails to comply with the requirements for interfaces laid down in this Regulation, the CBK shall ensure that the provision of PISs and AISs is not prevented or disrupted to the extent that the respective providers of such services comply with the conditions defined under Article 34 paragraph 5.

Article 32
Access interface options

ASPSPs shall establish the interface(s) referred to in Article 31 of this regulation by means of a dedicated interface or by allowing the use by the PSPs referred to in Article 31 paragraph 1 of this regulation of the interfaces used for authentication and communication with the ASPSP's PSUs.

Article 33
Obligations for a dedicated interface

1. Subject to compliance with Articles 31 and 32 of this regulation, ASPSPs 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 PSU for directly accessing its payment account online.
2. ASPSPs 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 PSUs both in terms of availability and of data provided in accordance with Article 37. Those interfaces, indicators and targets shall be monitored by the CBK and stress-tested.
3. ASPSPs that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of PISs and AISs. Such obstacles, may include, among others, preventing the use by PSPs referred to in Article 31 paragraph 1 of the credentials issued by ASPSPs to their customers, imposing redirection to the ASPSP's authentication or other functions, requiring additional authorizations and registrations in addition to those provided for in Articles 15 and 19 of the Law on Payment Services, or requiring additional checks of the consent given by PSUs to providers of PIS and AISs.
4. For the purpose of paragraphs 1 and 2 of this article, ASPSPs shall monitor the availability and performance of the dedicated interface. ASPSPs shall publish on their website quarterly statistics on the availability and performance of the dedicated interface and of the interface used by its PSUs.

Article 34
Contingency measures for a dedicated interface

1. ASPSPs shall include, in the design of the dedicated interface, a strategy and plans for contingency measures for the event that the interface does not perform in compliance with Article 33 of this regulation, that there is unplanned unavailability of the interface and that there is a systems 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 PISs or AISs are not replied to within 30 seconds.
2. Contingency measures shall include communication plans to inform PSPs making use of the dedicated interface of measures to restore the system and a description of the immediately available alternative options PSPs may have during this time.
3. Both the ASPSP and the PSPs referred to in Article 31 paragraph 1 shall report problems with dedicated interfaces as described in paragraph 1 of this article to the CBK without delay.
4. As part of a contingency mechanism, PSPs referred to in Article 31 paragraph 1 shall be allowed to make use of the interfaces made available to the PSUs for the authentication and communication

with their ASPSPs, until the dedicated interface is restored to the level of availability and performance provided for in Article 33 of this regulation.

5. For this purpose, ASPSPs shall ensure that the PSPs referred to in Article 31 paragraph 1 of this regulation can be identified and can rely on the authentication procedures provided by the ASPSP to the PSU. Where the PSPs referred to in Article 31 paragraph 1 of this regulation make use of the interface referred to in paragraph 4 of this article they shall:
   5.1. 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 PSU;
   5.2. continue to comply with the obligations following from Article 66 paragraph 3 and Article 67 paragraph 2 of the Law on Payment Services respectively;
   5.3. log the data that are accessed through the interface operated by the ASPSP for its PSUs, and provide, upon request and without undue delay, the log files to the CBK;
   5.4. duly justify to the CBK, upon request and without undue delay, the use of the interface made available to the PSUs for directly accessing its payment account online;
   5.5. inform the ASPSP accordingly.
6. The CBK shall, after having given due consideration to guidance and guidelines from the EBA or other European Union institutions as applicable to ensure a consistent application of the following conditions, exempt the ASPSPs that have opted for a dedicated interface from the obligation to set up the contingency mechanism described under paragraph 4 where the dedicated interface meets all of the following conditions:
   6.1. it complies with all the obligations for dedicated interfaces as set out in Article 33 of this regulation;
   6.2. it has been designed and tested in accordance with Article 31 paragraph 7 of this regulation to the satisfaction of the PSPs referred to therein;
   6.3. it has been widely used for at least 3 months by PSPs to offer AISs, PISs and to provide confirmation on the availability of funds for card-based payments;
   6.4. any problem related to the dedicated interface has been resolved without undue delay.
7. The CBK shall revoke the exemption referred to in paragraph 6 of this article where the conditions in subparagraphs 6.1 and 6.4 are not met by the ASPSPs for more than 2 consecutive calendar weeks. The CBK shall ensure that the ASPSP establishes, within the shortest possible time and at the latest within 2 months, the contingency mechanism referred to in paragraph 4 of this article.

Article 35
Certificates

1. For the purpose of identification, as referred to in Article 31 paragraph 1 subparagraph 1.1 of this regulation, PSPs shall rely on qualified certificates for electronic seals and signatures or qualified certificates for authentication of websites, according to the provisions in the legislation on electronic identification and trusted services on electronic transactions (Law No. 08/L – 022).
2. For the purpose of this Regulation, unique identification number or registration number as referred to in the official records in accordance with legislation on electronic identification and trusted

services on electronic transactions (Law No. 08/L – 022), shall be the authorization number of the PSP issuing card-based payment instruments, the AISPs and PISPs, including ASPSPs providing such services, available in the public register pursuant to Article 19 of the Law on Payment Services or resulting from the license or authorization framework and rules applicable to other applicable PSPs, such as banks.

3. For the purposes of this Regulation, qualified certificates for electronic seals or for website authentication referred to in paragraph 1 shall include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following:

   3.1. the role of the PSP, which maybe one or more of the following:

      3.1.1. account servicing;

      3.1.2. payment initiation;

      3.1.3. account information;

      3.1.4. issuing of card-based payment instruments;

   3.2. Central Bank of Kosovo, where the PSP is registered.

4. The attributes referred to in paragraph 3 of this article shall not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

Article 36
Security of communication session

1. ASPSPs, PSPs issuing card-based payment instruments, AISPs and PISPs 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 recognized encryption techniques.

2. PSPs issuing card-based payment instruments, AISPs and PISPs shall keep the access sessions offered by ASPSPs as short as possible and they shall actively terminate any such session as soon as the requested action has been completed.

3. When maintaining parallel network sessions with the ASPSP, AISPs and PISPs shall ensure that those sessions are securely linked to relevant sessions established with the PSU(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.

4. AISPs, PISPs and PSPs issuing card-based payment instruments with the ASPSP shall contain unambiguous references to each of the following items:

   4.1. the PSU or users and the corresponding communication session in order to distinguish several requests from the same PSU or users;

   4.2. for PISs, the uniquely identified payment transaction initiated;

   4.3. 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.

5. ASPSPs, AISPs, PISPs and PSPs issuing card-based payment instruments shall ensure that where they communicate personalized security credentials and authentication codes, these are not readable, directly or indirectly, by any staff at any time.

6. In case of loss of confidentiality of personalized security credentials under their sphere of competence, those providers shall inform without undue delay the PSU associated with them and the issuer of the personalized security credentials.

Article 37
Data exchanges

1. ASPSPs shall comply with each of the following requirements:

   1.1. they shall provide AISPs with the same information from designated payment accounts and associated payment transactions made available to the PSU when directly requesting access to the account information, provided that this information does not include sensitive payment data;

   1.2. they shall, immediately after receipt of the payment order, provide PISPs with the same information on the initiation and execution of the payment transaction provided or made available to the PSU when the transaction is initiated directly by the latter;

   1.3. they shall, upon request, immediately provide PSPs 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.

2. In case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements, the ASPSP shall send a notification message to the PISP or the AISP and the PSP issuing card-based payment instruments which explains the reason for the unexpected event or error.

   2.1. where the ASPSP offers a dedicated interface in accordance with Article 33 of this regulation, the interface shall provide for notification messages concerning unexpected events or errors to be communicated by any PSP that detects the event or error to the other PSPs participating in the communication session.

3. AISPs 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.

4. PISPs shall provide ASPSPs with the same information as requested from the PSU when initiating the payment transaction directly.

5. AISPs shall be able to access information from designated payment accounts and associated payment transactions held by ASPSPs for the purposes of performing the AIS in either of the following circumstances:

   5.1. whenever the PSU is actively requesting such information;

   5.2. where the PSU does not actively request such information, no more than four times in a 24-hour period, unless a higher frequency is agreed between the AISP and the ASPSP, with the PSU's consent.

Article 38
Annex

This regulation is comprised of Annex 1 Reference fraud rate.

CHAPTER VI
FINAL PROVISIONS

Article 39
Enforcement, Improvement Measures and Penalties

Any violation of the provisions of this Regulation shall be subject to corrective measures and/or administrative and civil penalties as defined within article 67 of the Law No. 03/L-209 on Central Bank of the Republic of Kosovo, as amended and supplemented by Law No. 05/L –150 and article 124 of the Law No. 08/L-328 on Payment Services.

Article 40
Transitional Period

PSPs subject to this Regulation shall adapt their activities and operations to the provisions of this Regulation no later than 18 months after the date of entry into force provided for in the next Article.

Article 41
Entry into force

This Regulation shall enter into force 10 (ten) days after the entry into force of Law No. 08/L-328 on Payment Services.

Dr.sc. Bashkim Nurboja
Chairperson of the Board of Central Bank of the Republic of Kosovo

ANNEX 1

	Reference fraud rate (%) for:	
ETV	**Remote electronic card-based payments**	**Remote electronic credit transfers**
EUR 500	0,01	0,005
EUR 250	0,06	0,01
EUR 100	0,13	0,015