

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

(OGM 021/23 of 24 February 2023, 078/24 of 7 August 2024)

I BASIC PROVISIONS

Subject Matter

Article 1

This Decision prescribes security requirements to be met by the payment service providers for ensuring strong customer authentication and common and secure open standards for communication, as well as exemptions from the application of strong customer authentication requirements.

General authentication requirements

Article 2

- (1) A payment service provider shall have transaction monitoring mechanisms in place that enable them to detect unauthorised payment transactions or fraudulent payment transactions for the purpose of the implementation of the requirements referred to in Articles 5 to 22 of this Decision.
- (2) Monitoring mechanisms referred to in paragraph (1) of this Article shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials.
- (3) A payment service provider shall ensure that the monitoring mechanisms referred to in paragraph (1) of this Article 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 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 payment service user and the abnormal use of the access device or the software.

Audit of the security measures

Article 3

- (1) The implementation of the requirements set up in this Decision shall be documented, periodically tested, evaluated and audited in accordance with the law by independent internal or external auditors with expertise in IT security and payments.
- (2) The frequency of audits referred to in paragraph (1) of this Article shall be determined in accordance with the regulations governing the conditions and the method of auditing financial statements of the payment service providers.

- (3) By way of derogation from paragraph (2) of this Article, where the payment service provider does not apply strong customer authentication in accordance with Article 19 of this Decision, the payment service provider shall provide, at a minimum on yearly basis, audit of the methodology, models, calculated and reported fraud rates referred to in Article 20 of this Decision.
- (4) By way of derogation from paragraph (1) of this Article, during the first year of making use of the exemption referred to in Article 19 of this Decision and at least every 3 years thereafter, or more frequently at the request of the Central Bank of Montenegro (hereinafter: the Central Bank), the audit referred to in paragraph (3) of this Article shall be carried out by an independent and qualified external auditor.
- (5) The report containing the evaluation on the compliance of the payment service provider's security measures with the requirements set out in this Decision shall be drawn up after the audit conducted in accordance with the provisions of this Article.
- (5) The audit report referred to in paragraph (5) of this Article shall be made available to the Central Bank upon their request.

Meaning of terms

Article 4

The terms used in this Decision shall have the following meanings:

- 1) electronic payment transaction means a payment transaction initiated and executed in the manner which includes the use of electronic platforms or devices and does not include paper-based payment transactions, mail orders or telephone orders;
- 2) interface means a logical component of the system through which, in accordance with the pre-defined set of routines and protocols, establishes communication channel and exchanges of information with other systems;
- 3) credit transfer means a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provider which holds the payer's payment account, based on a payment order given by the payer;
- 4) online means the possibility of connecting provider and user of certain service via publicly available communication network (e.g. Internet);;
- 5) sensitive payment data means data, including personalised security credentials, which can be used to carry out fraud, whereas for the activities of payment initiation service provider and account information service provider, the name of the account owner and the account number do not constitute sensitive payment data;
- 6) personalised security credentials means personalised features provided by the payment service provider to a payment service user for the purposes of authentication;
- 7) payment card means a payment instrument enabling its holder to make payments for goods and services either at an accepting device or remotely, and/or to withdraw cash and/or use other services at an automated teller machine or another self-service device;
- 8) remote payment transaction means a payment transaction initiated via internet or through a device that can be used for distance communication;
- 9) strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge, possession and inherence that are independent and that only user knows and possesses, which means that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

II SECURITY REQUIREMENTS FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

Authentication code

Article 5

- (1) Strong customer authentication shall be performed using two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.
- (2) The authentication code referred to in paragraph (1) of this Article 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 action through a remote channel which may imply a risk of payment fraud or other abuses.
- (3) For the purpose of acting in accordance with paragraphs (1) and (2) of this Article, a payment service provider shall adopt security measures ensuring that:
 - 1) no information on any of the elements referred to in paragraph (1) of this Article 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.
- (4) A payment service provider shall ensure that the strong customer authentication by means of generating an authentication code includes the following measures:
 - 1) where the strong customer authentication has failed to generate an authentication code referred to in paragraph (1) of this Article, it shall not be possible to identify which of the elements referred to in paragraph (1) of this Article was incorrect;
 - 2) the number of failed authentication attempts that can take place consecutively, after which the actions for which the strong customer authentication is carried out shall be temporarily or permanently blocked, shall not exceed five within a given period of time;
 - 3) the communication sessions are protected against the capture of strong customer authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements referred to in Articles 29 to 37 of this Decision;
 - 4) the maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed five minutes.
- (5) Where the block referred to in paragraph (4) item 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 2 paragraph (3) of this Decision.
- (6) The payment service provider shall alert the payer before the temporary block referred to in paragraph (4) item 2) of this Article is made permanent.
- (7) Where the temporary block referred to in paragraph (4) item 2) of this Article has been made permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments.

Dynamic linking

Article 6

- (1) Where a payment service provider applies strong customer authentication in the case of initiating remote electronic payment transaction, in addition to the requirements of Article 5 of this Decision, they shall also adopt security measures ensuring that:
 - 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.
- (2) For the purpose of acting in accordance with paragraph (1) of this Article, payment service provider shall adopt security measures which ensure the confidentiality, authenticity and integrity of:
- 1) the amount of the payment transaction and the payee throughout all of the phases of the strong customer authentication;
 - 2) the information displayed to the payer throughout all of the phases of the strong customer authentication including the generation, transmission and use of the authentication code.
- (3) For the purpose of acting in accordance with paragraph (1) item 2) of this Article 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 37a paragraph (1) of the Payment System Law (hereinafter: 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

Article 7

- (1) A payment service provider 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.
- (2) The use by the payer of elements referred to in paragraph (1) of this Article shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.

Requirements of the elements categorised as possession

Article 8

- (1) 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.
- (2) The use of elements referred to in paragraph (1) of this Article by the payer shall be subject to mitigation measures designed to prevent replication of the elements.

Requirements of devices and software linked to elements categorised as inherence

Article 9

- (1) A payment service provider shall adopt measures to mitigate the risk that the elements for strong customer authentication categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties.
- (2) The payment service provider shall ensure, at a minimum, that access devices and software referred to in paragraph (1) of this Article have a very low probability of an unauthorised party being authenticated as the payer.

- (3) The use of the elements referred to in paragraph (1) of this Article by the payer shall be subject to measures ensuring that those devices and the software guarantee resistance against unauthorised use of the elements through access to the devices and the software.

Independence of the elements for strong customer authentication

Article 10

- (1) A payment service provider shall ensure that the use of the elements of strong customer authentication referred to in Articles 7, 8 and 9 of this Decision 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) The payment service provider 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 payment service provider shall establish 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 have taken place, mechanisms to mitigate the consequences thereof.

III EXEMPTIONS FROM THE APPLICATION OF REQUIREMENTS FOR STRONG CUSTOMER AUTHENTICATION

Payment account information

Article 11

- (1) A payment service provider shall be allowed not to apply strong customer authentication, subject to compliance with the general requirements laid down in Article 2 of this Decision, where a payment service user 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) the balance of one or more designated payment accounts; or
 - 2) the payment transactions executed in the last 90 days through one or more designated payment accounts.
- (2) The exemptions from the application of strong customer authentication referred to in paragraph (1) of this Article shall not be applied where:
- 1) the payment service user is accessing online the information specified in paragraph (1) of this Article for the first time; or
 - 2) more than 180 days have elapsed since the last time the payment service user accessed online the information specified in paragraph (1) item 2) of this Article, and strong customer authentication was applied.

Access to the payment account information through an account information service provider

Article 11a

- (1) A payment service provider shall not apply strong customer authentication where a payment service user is accessing its payment account online through an account information service provider, provided that access is limited to one of the following items online without disclosure of sensitive payment data:
- 1) the balance of one or more designated payment accounts; or

- 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) of this Article, payment service provider shall apply strong customer authentication where:
 - 1) the payment service user is accessing online the information specified in paragraph (1) of this Article for the first time through the account information service provider; or
 - 2) more than 180 days have elapsed since the last time the payment service user accessed online the information specified in paragraph (1) of this Article through the account information service provider and strong customer authentication was applied.
- (3) By way of derogation from paragraph (1) of this Article, payment service provider shall be allowed to apply strong customer authentication where they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account.
- (4) In the case referred to in paragraph (3) of this Article, the payment service provider shall document and duly justify to the Central Bank, upon request, the reasons for applying strong customer authentication.
- (5) An account servicing payment service provider that offers a dedicated interface as referred to in Article 32 of this Decision shall not be required to implement the exemption laid down in paragraph (1) of this Article for the purpose of the contingency mechanism referred to in Article 34 paragraphs (5) and (6) of this Decision, where they do not apply the exemption laid down in Article 11 of this Decision in the direct interface used for authentication and communication with their payment service users.

Contactless payments at point of sale

Article 12

A payment service provider shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 of this Decision, where the payer initiates a contactless electronic payment transaction and where:

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

Unattended terminals for transport fares and parking fees

Article 13

A payment service provider shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 of this Decision, 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

Article 14

- (1) A payment service provider shall apply strong customer authentication where a payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider.

- (2) The payment service provider shall be allowed not to apply strong customer authentication, subject to compliance with the general requirements referred to in Article 2 of this Decision, where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries referred to in paragraph (1) of this Article previously created by the payer.

Recurring transactions

Article 15

- (1) A payment service provider 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) The payment service provider shall be allowed not to apply strong customer authentication, subject to compliance with the general requirements referred to in Article 2 of this Decision, for the initiation of all subsequent payment transactions included in the series of payment transactions referred to in paragraph (1) of this Article.

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

Article 16

A payment service provider shall be allowed not to apply strong customer authentication, subject to compliance with the general requirements laid down in Article 2 of this Decision, 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 account servicing payment service provider.

Low-value transactions

Article 17

A payment service provider shall be allowed not to apply strong customer authentication, where the payer initiates a remote electronic payment transaction and where:

- 1) the amount of the remote electronic payment transaction does not exceed EUR 30; 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 EUR 100; 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

Article 18

A payment service provider 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 Central Bank is satisfied that those processes or protocols guarantee at least equivalent levels of security to those provided for by the Law.

Transaction risk analysis

Article 19

- (1) A payment service provider 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 Article 2 of this Decision.

- (2) An electronic payment transaction referred to in paragraph (1) of this Article shall be considered as posing a low level of risk where the following requirements are met:
 - 1) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 20 of this Decision, is equivalent to or below the reference fraud rates specified in Annex 1 which is an integral part of this Decision;
 - 2) the amount of the transaction does not exceed the relevant exemption threshold value ('ETV') specified in Annex 1 of this Decision;
 - 3) the payment service provider as a result of performing a real time risk analysis has 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 customer authentication procedure;
 - known fraud scenario in the provision of payment services;
 - abnormal location of the payer;
 - high-risk location of the payee.
- (3) The payment service provider that intends to exempt remote electronic payment transactions referred to in paragraph (1) of this Article from strong customer authentication on the ground that they pose a low risk shall take into account in particular the following risk-based factors:
 - 1) the previous spending patterns of the individual payment service user;
 - 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 payment service user in relation to the user's payment transaction history.
- (4) The assessment made by a payment service provider shall combine all those risk-based factors referred to in paragraph (3) of this Article 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

Article 20

- (1) The payment service provider shall ensure that the overall fraud rates for the remote electronic card-based payments and remote electronic credit transfers covering payment transactions authenticated through strong customer authentication and those executed under any of the exemptions referred to in Articles 14 to 19 of this Decision are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction indicated in the Annex 1 of this Decision.
- (2) The overall fraud rate for each type of transaction referred to in paragraph (1) of this Article shall be calculated as the total value of remote unauthorised transactions or remote fraudulent transactions, whether the funds have been recovered or not, divided by the total value of all remote payment 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 Decision on a rolling quarterly basis (90 days).
- (3) The methodology and any model, used by the payment service provider to calculate the fraud rates referred to in paragraph (1) of this Article, as well as the fraud rates themselves, shall be adequately documented and made fully available to the Central Bank, upon their request.

Cessation of exemptions based on transaction risk analysis

Article 21

- (1) A payment service provider that does not apply strong customer authentication referred to in Article 19 of this Decision shall immediately report to the Central Bank where one of their monitored fraud rates, for any type of payment transactions indicated in the Annex 1 of this Decision, exceeds the applicable reference fraud rate and shall provide a description of the measures that they intend to adopt to restore compliance of their monitored fraud rate with the applicable reference fraud rates.
- (2) The payment service provider referred to in paragraph (1) of this Article shall immediately cease to apply strong customer authentication for any type of payment transactions indicated in the Annex 1 of this Decision in the specific exemption threshold range where their monitored fraud rate exceeds for two consecutive quarters the reference fraud rate applicable for that payment instrument or type of payment transaction in that exemption threshold range.
- (3) In the case of paragraph (2) of this Article, payment service provider shall use the 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.
- (4) Where the payment service provider intends to cease the application of strong customer authentication referred to in Article 19 of this Decision, they shall notify the Central Bank in a reasonable timeframe and shall 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.

Monitoring of payment transactions

Article 22

- (1) The payment service provider that does not apply strong customer authentication set out in Articles 11 to 19 of this Decision 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 payment transactions or fraudulent payment transactions in accordance with the provisions of Article 30 of the Law, 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 of this Decision;
 - 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 of this Decision;
 - 3) for each of the exemptions applied in accordance with the provisions of this Decision, 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) The payment service provider shall make the results of the monitoring in accordance with paragraph (1) of this Article available to the Central Bank, upon their request.

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

General requirements for confidentiality and integrity of the personalised security credentials

Article 23

- (1) Payment service provider shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication.
- (2) For the purpose of acting in accordance with paragraph (1) of this Article, the payment service provider shall ensure that 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 payment service 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.
- (3) The payment service provider shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.
- (4) The payment service provider shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Articles 5 to 10 of this Decision take place in secure environments in accordance with strong and widely recognised industry standards.

Creation and transmission of personalised security credentials

Article 24

- (1) A payment service provider shall ensure that the creation of personalised security credentials is performed in a secure environment.
- (2) The payment service provider shall 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.

Association with the payment service user

Article 25

- (1) A payment service provider shall ensure that only the payment service user is associated, in a secure manner, with the personalised security credentials, the customer authentication devices and the software.
- (2) For the purpose of acting in accordance with paragraph (1) of this Article, payment service provider shall ensure that the following requirements is met:
 - 1) the association of the payment service user's identity with personalised security credentials, customer 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 other similar 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 payment service user's identity with the personalised security credentials and with customer authentication devices and software is performed using strong customer authentication.

Delivery of personalised security credentials, authentication devices and software

Article 26

- (1) A payment service provider shall ensure that the delivery of personalised security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorised use due to their loss, theft or copying.
- (2) For the purpose of acting in accordance with paragraph (1) of this Article, payment service provider 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 payment service user;
 - 2) mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user by means of the internet;
 - 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 and 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 Article 25 of this Decision.

Renewal of personalised security credentials

Article 27

A payment service provider shall ensure that the renewal or re-activation of personalised security credentials adhere to the procedures for the creation, association and delivery of the personalised security credentials and of the authentication devices in accordance with Articles 24, 25 and 26 of this Decision.

Destruction, deactivation and revocation

Article 28

A payment service provider shall ensure that they have effective processes in place to apply 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 payment services 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 registries.

V COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION

1. General requirements for communication

Requirements for identification

Article 29

- (1) A payment service provider 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) The payment service provider shall 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

Article 30

- (1) A payment service provider shall have processes in place which ensure that all payment transactions and other interactions with the payment services 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 payment transaction in all the various stages.
- (2) For the purpose of acting in accordance with paragraph (1) of this Article, payment service provider shall ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies on the following:
 - 1) a unique identifier of the session;
 - 2) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data;
 - 3) timestamps which shall be based on a unified time-reference system and which shall be synchronised according to an official time signal.

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

General requirements for access interfaces

Article 31

- (1) An account servicing payment service provider that offers to a payer a payment account that is accessible online shall have in place at least one interface which meets 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;
 - 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.
- (2) For the purposes of authentication of the payment service user, the interface referred to in paragraph (1) of this Article 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 payment service user.

- (3) The interface referred to in paragraph (1) of this Article 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 payment service user;
 - 2) communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and any payment service user concerned shall be established and maintained throughout the authentication;
 - 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.
- (4) Account servicing payment service provider shall ensure that their interfaces referred to in paragraph (1) of this Article follow standards of communication which are issued by international or European standardisation organisations.
- (5) Account servicing payment service provider shall also ensure that the technical specification of any of the interfaces referred to in paragraph (1) of this Article is documented specifying a set of routines, protocols, and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments for allowing their software and applications to interoperate with the systems of the account servicing payment service providers.
- (6) Account servicing payment service provider shall, before the application date of the access interface referred to in paragraph (1) of this Article, make the documentation referred to in paragraph (5) of this Article available, at no charge, upon request by authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or payment service providers that have applied to the Central Bank for the relevant authorisation, and shall make a summary of the documentation publicly available on their website.
- (7) Account servicing payment service provider shall ensure that, except for emergency situations, any change to the technical specification referred to in paragraph (5) of this Article is made available to authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, or payment service providers that have applied to the Central Bank for the relevant authorisation, in advance as soon as possible and not less than three months before the change is implemented.
- (8) By way of derogation from paragraph (7) of this Article, account servicing payment service provider shall make available to the payment service providers referred to in paragraph (7) of this Article the changes made to the technical specifications of their interfaces in order to comply with Article 11a of this Decision not less than 2 months before such changes are implemented.
- (9) Payment service provider shall document emergency situations referred to in paragraph (7) of this Article where changes to the technical specification referred to in paragraph (5) of this Article were implemented and make the documentation available to the Central Bank on request.
- (10) Account servicing payment service provider shall make available a testing facility, including support, for connection and functional testing to enable authorised payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers, or payment service providers that have applied to the Central Bank for the relevant authorisation, to test their software and applications used for offering a payment service to users.
- (11) The testing facility referred to in paragraph (10) of this Article should enable testing of the interface in the manner specified in item 5.5 of Annex 2 which is an integral part of this Decision and it should be made available before the application date of the access interface referred to in paragraph (1) of this Article.
- (12) The testing facility referred to in paragraph (10) of this Article shall not be used for sharing sensitive information, in particular for sharing sensitive payment data.

- (13) In the event that an account servicing payment services provider fails to comply with the requirements set out in this Decision for interfaces referred to in paragraph (1) of this Article, they shall ensure that the provision of payment initiation services and account information services is not prevented or disrupted to the extent that the respective providers of such services comply with the requirements referred to in Article 34 paragraphs (6) and (7) of this Decision.

Access interface options

Article 32

Account servicing payment service provider shall establish one or more interfaces referred to in Article 31 of this Decision by means of a dedicated interface or by allowing the use by the payment service providers referred to in Article 31 paragraph (1) of this Decision of the interfaces used for customer authentication and communication with the account servicing payment service provider's payment services users.

Obligations for a dedicated interface

Article 33

- (1) Notwithstanding the provisions of Articles 31 and 32 of this Decision, the account servicing payment service provider that has 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 payment service users for directly accessing its payment accounts online.
- (2) Account servicing payment service provider that has 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 exchanged in accordance with Article 37 of this Decision.
- (3) Payment service provider shall perform stress-tests of the dedicated interface referred to in paragraph (2) of this Article.
- (4) Account servicing payment service provider that has 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.
- (5) Obstacles referred to in paragraph (4) of this Article, shall include, in particular, preventing the use by payment service providers referred to in Article 31 paragraph (1) of this Decision 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 in the Law, or requiring additional checks of the consent given by payment service users to payment initiation service providers and account information service providers.
- (6) For the purpose of acting in accordance with paragraphs (1) and (2) of this Article, the account servicing payment service provider shall monitor the availability and performance of the dedicated interface, and publish on its website quarterly statistics on the availability and performance of the dedicated interface and of the interface used by its payment service users.

Contingency measures for a dedicated interface

Article 34

- (1) Account servicing payment service provider 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 Decision, that there is unplanned unavailability of the interface or that there is a systems breakdown.
- (2) Unplanned unavailability or a systems breakdown within the meaning of paragraph (1) of this Article may be presumed to have arisen when five consecutive requests for access to information

for the provision of payment initiation service or account information service are not replied to within 30 seconds.

- (3) Contingency measures referred to in paragraph (1) of this Article 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 use during this time.
- (4) Both the account servicing payment service providers and the payment service providers referred to in Article 31 paragraph (1) of this Decision shall report problems with dedicated interfaces referred to in paragraphs (1) and (2) of this Article to the Central Bank without delay.
- (5) Account servicing payment service provider shall establish a contingency mechanism, which shall allow the payment service providers referred to in Article 31 paragraph (1) of this Decision to make use of the interfaces made available to its payment service users for the customer 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 of this Decision.
- (6) For the purpose of acting in accordance with paragraph (5) of this Article, the account servicing payment service provider shall ensure that the payment service providers referred to in Article 31 paragraph (1) of this Decision can be identified and can use the authentication procedures provided by the account servicing payment service provider to the payment service user.
- (7) Where the payment service providers referred to in Article 31 paragraph (1) of this Decision make use of the interface referred to in paragraph (5) of this Article 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 payment service user;
 - 2) ensure compliance with the rules referred to in Article 30b paragraph (4) and Article 30c paragraph (3) 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 Central Bank;
 - 4) duly justify to the Central Bank, upon request and without undue delay, the use of the interface made available to the payment service users for directly accessing their payment accounts online;
 - 5) notify the account servicing payment service provider on the use of the interface accordingly.
- (8) The Central Bank may exempt the account servicing payment service provider that has opted for a dedicated interface from the obligation to set up the contingency mechanism referred to in paragraph (5) of this Article, where, on the basis of information and data provided by that payment service provider, it establishes that:
 - 1) it meets the requirements referred to in Article 33 of this Decision and additional requirements set out in Annex 2 to this Decision;
 - 2) the dedicated interface has been designed and tested in accordance with Article 31 paragraphs (10), (11), and (12) of this Decision to the satisfaction of the payment service providers referred to in Article 31 paragraph (10) of this Decision;
 - 3) the interface has been used for at least three 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; and
 - 4) any problem related to the dedicated interface has been resolved without undue delay.
- (9) Where the payment service provider referred to in paragraph (8) of this Article fails to meet the conditions referred to in items 1) and 4) of that Article for more than 14 consecutive days, it shall establish the contingency mechanism referred to in paragraph (5) of this Article no later than within 2 months from the date the non-compliance with those conditions was identified.

Certificates

Article 35

- (1) For the purpose of identification, as referred to in Article 31 paragraph (1) of this Decision, payment service providers shall use qualified certificates for electronic seals or qualified certificates for website authentication in accordance with the law governing electronic identification and electronic signature, which, in a language customary in the sphere of international finance, shall contain the following:
- 1) the role of the payment service provider, which maybe one or more of the following:
 - account servicing;
 - payment initiation;
 - account information; and/or
 - issuing of card-based payment instruments;
 - 2) the name of the competent authority which granted the authorisation to the payment service provider.

Security of communication session

Article 36

- (1) Account servicing payment service providers, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers 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 widely recognised encryption techniques.
- (2) Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the access sessions offered by account servicing payment service providers as short as possible and they shall actively terminate any such session as soon as the requested action has been completed.
- (3) 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 payment service user(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.
- (4) Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments with the account servicing payment service provider shall contain unambiguous references to each of the following items:
- 1) the payment service user or users and the corresponding communication session in order to distinguish several requests from the same payment service 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.
- (5) 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, directly or indirectly, by any employee or another person hired by those payment service providers at any time.
- (6) In case of loss of confidentiality of personalised security credentials under their sphere of competence, payment service providers referred to in paragraph (5) of this Article shall inform without undue delay the payment services user and the issuer of the personalised security credentials.

Data exchanges

Article 37

- (1) Account servicing payment service providers shall:
 - 1) provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data;
 - 2) immediately after receipt of the payment order, provide payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the payment transaction is initiated directly by the latter;
 - 3) 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.
- (2) In case of an unexpected event or error occurring during the process of identification, customer 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.
- (3) Where the account servicing payment service provider offers a dedicated interface in accordance with Article 33 of this Decision, 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.
- (4) Account information service providers shall have in place suitable and effective mechanisms that prevent access to information other than information from designated payment accounts and associated payment transactions, in accordance with the user's explicit consent.
- (5) Payment initiation service providers shall provide account servicing payment service provider with the same information as requested from the payment service user when initiating the payment transaction directly.
- (6) Account information service providers may 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 the following circumstances:
 - 1) whenever the payment service user is actively requesting such information;
 - 2) where the payment service user does not actively request such information, no more than four times in a 24-hour period, unless a higher frequency is agreed between the account information service provider and the account servicing payment service provider, with the payment service user's consent.

VI. FINAL PROVISION

Entry into force

Article 38

This Decision shall enter into force on the eight day following that of its publication in the Official Gazette of Montenegro.

THE COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

ANNEX 1

Exemption threshold value (ETV)	Reference fraud rate (%) for:	
	Remote electronic card-based payment transactions	Remote electronic credit transfers
EUR 500	0,01	0,005
EUR 250	0,06	0,01
EUR 100	0,13	0,015

ANNEX 2

Additional requirements for the exemption from the obligation to set up a contingency mechanism referred to in Article 34 paragraph (5) of this Decision

To be eligible for the exemption from the obligation to set up a contingency mechanism referred in Article 34 paragraph (5) of this Decision, the account servicing payment service provider must meet the following additional requirements:

1. Service level, availability and performance requirements

- 1.1 When determining the service level targets referred to in Article 33 paragraph (2) of this Decision, the account servicing payment service provider shall also determine the requirements for problem resolution, out of hours support, monitoring, contingency plans and maintenance for its dedicated interface, that are at least as stringent as those for the interface(s) made available to its own payment service users.
- 1.2 In terms of the availability of the dedicated interface, the account servicing payment service provider should define at a minimum the following key performance indicators:
 - 1) the uptime per day of each interface; and
 - 2) the downtime per day of each interface.
- 1.3 In terms of the performance of the dedicated interface, the account servicing payment service provider should define at a minimum the following key performance indicators:
 - 1) the daily average time (in milliseconds) taken, per request, for the account servicing payment service provider to provide the payment initiation service provider with all the information requested in accordance with Article 30b paragraph (5) of the Law and Article 37 paragraph (1) item 2) of this Decision;
 - 2) the daily average time (in milliseconds) taken, per request, for the account servicing payment service provider to provide the account information service provider with all the information requested in accordance with Article 37 paragraph (1) item 1) of this Decision;
 - 3) the daily average time (in milliseconds) taken, per request, for the account servicing payment service provider to provide the payment service provider issuing card-based payment instruments or the payment initiation service provider with a 'yes/no' confirmation in accordance with Article 30a paragraph (3) of the Law and Article 37 paragraph (1) item 3) of this Decision;
 - 4) the daily error response rate – calculated as the number of error messages concerning errors attributable to the account servicing payment service provider sent by the account servicing payment service provider to the payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments in accordance with Article 37 paragraph (2) of this Decision per day, divided by the number of requests received by the account servicing payment service provider from payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments in the same day.

1.4 For the purpose of calculating the availability indicators set out in item 1.2 of this Annex for the dedicated interface, the account servicing payment service provider should:

- 1) calculate the percentage uptime as 100% minus the percentage downtime;
- 2) calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24-hour period, starting and ending at midnight;
- 3) count the interface as 'down' when five consecutive requests for access to information for the provision of payment initiation service, account information service or confirmation of availability of funds are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple payment initiation service providers, account information service providers or payment service providers issuing card-based payment instruments. In such a case, the account servicing payment service provider should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided.

2. Requirements for publication of statistics

2.1 For the purpose of meeting the conditions referred to in Article 33 paragraph (6) of this Decision, the account servicing payment service provider shall provide the Central Bank with a plan for publication of daily statistics on a quarterly basis on the availability and performance of the dedicated interface as set out in items 1.2 and 1.3 of this Annex, and of each of the interfaces made available to its own payment service users for directly accessing their payment accounts online, together with information on where these statistics will be published and the date of first publication.

2.2 The publication of statistics in accordance with item 2.1 of this Annex should enable payment initiation service providers, account information service providers, payment service providers issuing card-based payment instruments and payment service users to compare the availability and performance of the dedicated interface with the availability and performance of each of the interfaces made available by the account servicing payment service provider to its payment service users for directly accessing their payment accounts online on a daily basis.

3. Requirements for dedicated interface stress testing

3.1 For the purpose of the dedicated interface stress testing, the account servicing payment service provider should have in place processes to establish and assess how the dedicated interface performs when subjected to an extremely high number of requests from payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, in terms of the impact that such stresses have on the availability and performance of the dedicated interface and the defined service level targets.

3.2 The stress testing of the dedicated interface should include but not be limited to:

- 1) the capability to support access by multiple payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments;
- 2) the capability to deal with an extremely high number of requests from payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, in a short period of time without failing;
- 3) the use of an extremely high number of concurrent sessions open at the same time for payment initiation, account information and confirmation of availability of funds requests; and
- 4) requests for large volumes of data.

3.3 The account servicing payment service provider should provide the Central Bank with a summary of the results of the stress tests, including the assumptions used as a basis for stress testing each of the elements referred to in item 3.2 of this Annex and how any issues identified have been addressed.

4. Requirements regarding obstacles

- 4.1 The account servicing payment service provider shall provide the Central Bank with the following:
- 1) a summary of the methods of carrying out the authentication procedures of the payment service users that are supported by the dedicated interface, i.e. redirection, decoupled, embedded or a combination thereof; and
 - 2) an explanation of the reasons why the methods referred to in sub-item 1 of this item are not obstacles within the meaning of Article 33 paragraphs (4) and (5) of this Decision, and how such methods allow payment initiation service providers and account information service providers to rely on all the customer authentication procedures provided by the account servicing payment service provider to its payment service users, together with evidence that the dedicated interface does not give rise to unnecessary delay or difficulties and does not have an adverse effect on their satisfaction when accessing their account via a payment initiation service provider, account information service provider or payment service provider issuing card-based payment instruments or to any other attributes, including unnecessary or superfluous steps or the use of unclear or discouraging language, that would directly or indirectly dissuade the payment service users from using the services of payment initiation service providers, account information service providers or payment service providers issuing card-based payment instruments.
- 4.2 The explanation referred to in item 4.1 sub-item 2 of this Annex should include a confirmation that:
- 1) the dedicated interface does not prevent payment initiation service providers and account information service providers from relying upon the customer authentication procedures provided by the account servicing payment service provider to its payment service users;
 - 2) no additional authorisations or registrations are required from payment initiation service providers, account information service providers or payment service providers issuing card-based payment instruments, other than those imposed in the Law;
 - 3) there are no additional checks by the account servicing payment service provider on the consent, as referred to in Article 33 paragraph (5) of this Decision, given by the payment service users to the payment initiation service provider or account information service provider to access the information on the payment accounts held with the account servicing payment service provider or to initiate payments.

5. Requirements regarding the design and testing to the satisfaction of payment service providers

- 5.1 The account servicing payment service provider shall provide the Central Bank with the following:
- 1) evidence that the dedicated interface meets the prescribed conditions for access and data, in particular the following:
 - a description of the functional and technical specifications that the account servicing payment service provider has implemented;
 - a summary of how the implementation of these specifications fulfils the prescribed requirements; and
 - 2) information on whether, and if so how, the account servicing payment service provider has engaged with payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments.
- 5.2 Where the account servicing payment service provider is implementing a standard developed by a market initiative:
- 1) the information referred to in item 5.1 sub-item 1 indent 1 of this Annex may consist of information regarding which market initiative standard the account servicing payment service

- provider is implementing, whether or not it has deviated in any specific aspect from such standard, and if so, how it has deviated and how it meets the prescribed requirements;
- 2) the information referred to in item 5.1 sub-item 1 indent 2 of this Annex may include, where available, the results of the conformance testing developed by the market initiative, attesting compliance of the interface with the respective market initiative standard.
- 5.3 Within the meaning of item 5.2 sub-item 2 of this Annex, a market initiative means a group of stakeholders that have developed functional and technical specifications for dedicated interfaces and, in doing so, have obtained input from payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments.
- 5.4. For the purpose of determining the fulfilment of condition referred to in Article 34 paragraph (8) item 2) of this Decision, the account servicing payment service provider shall provide evidence to the Central Bank that it has, in accordance with Article 31 paragraphs (6) and (7) of this Decision, made the technical specifications of the dedicated interface available to authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or a person that has applied to the Central Bank for the authorisation to provide any of these services, at a minimum, publishing a summary of the specification of the dedicated interface on its website in accordance with Article 31 paragraph (6) of this Decision.
- 5.5 The testing facility should allow account servicing payment service providers, authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or a person that has applied to the Central Bank for the authorisation to provide any of these services, to test the dedicated interface in a secure, dedicated testing environment with non-real payment service users data, for the following:
- 1) a stable and secure connection;
 - 2) the ability of account servicing payment service providers and authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments to exchange the relevant certificates in accordance with Article 35 of this Decision;
 - 3) the ability to send and receive error messages in accordance with Article 37 paragraph (2) of this Decision;
 - 4) the ability of payment initiation service providers to send, and of account servicing payment service providers to receive, payment initiation orders, and the ability of account servicing payment service providers to provide the information requested in accordance with Article 30b paragraph (5) item 2) of the Law and Article 37 paragraph (1) item 2) of this Decision;
 - 5) the ability of account information service provider to send, and of account servicing payment service providers to receive, requests for access to payment account data, and the ability of account servicing payment service providers to provide the information requested in accordance with Article 37 paragraph (1) item 1) of this Decision;
 - 6) the ability of payment service providers issuing card-based payment instruments and payment initiation service providers to send, and of account servicing payment service providers to receive, requests from payment service providers issuing card-based payment instruments and payment initiation service providers and the ability of the account servicing payment service provider to send a 'yes/no' confirmation to payment service providers issuing card-based payment instruments and payment initiation service providers in accordance with Article 37 paragraph (1) item 3) of this Decision; and
 - 7) the ability of payment initiation service providers and account information service providers to rely on all the authentication procedures provided by the account servicing payment service provider to its payment service users.
- 5.6. The account servicing payment service provider shall provide the Central Bank with a summary of the results of the testing referred to in Article 31 paragraph (10) of this Decision, for each of the elements to be tested in accordance with item 5.5 sub-items 1 to 7 of this Annex, including the

number of payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments that have used the testing environment, the feedback received by the account servicing payment service provider from these payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, the data on issues identified and a description of how these issues have been addressed.

5.7 For the purpose of assessing whether the condition referred to in Article 34 paragraph (8) item 2) of this Decision has been met, any problems reported to the Central Bank by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments in relation to item 5.5 of this Annex may also be taken into account.

6. Requirements regarding the wide usage of the interface

6.1 For the purposes of evidencing compliance with the condition referred to in Article 34 paragraph (8) item 3) of this Decision, the account servicing payment service provider shall provide the Central Bank with the following:

1) a description of the usage of the dedicated interface for the period referred to in Article 34 paragraph (8) item 3) of this Decision, including but not limited to:

- information on the number of payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments that have used the interface to provide services to customers; and
- information on the number of requests sent by those payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments to the account servicing payment service provider via the dedicated interface that have been replied to by the account servicing payment service provider;

2) evidence that the account servicing payment service provider has made all reasonable efforts to ensure wide usage of the dedicated interface, including by communicating its availability via appropriate channels, including, where relevant, the website of the account servicing payment service provider, social media, industry trade bodies, and cooperation with market participants.

6.2 When assessing whether the condition referred to in Article 34 paragraph (8) item 3) of this Decision has been met, the information delivered to the Central Bank in accordance with items 5 and 7 of this Annex may also be taken into account.

6.3 The three-month period referred to in Article 34 paragraph (8) item 3) of this Decision may run concurrently with the testing referred to in Article 31 paragraph (10) of this Decision.

7. Requirements regarding the resolution of problems

7.1 For the purposes of evidencing compliance with the condition referred to in Article 33 paragraph (8) item 4) of this Decision, the account servicing payment service provider shall provide the Central Bank with the following:

1) information on the systems or procedures in place for tracking and resolving problems, particularly those reported by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments; and

2) an explanation of the problems, particularly those reported by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, that have not been resolved in accordance with the service level targets set out in item 1.1 of this Annex.