APPENDIX No. 14

to the Agreement on complex banking services for legal entities and individual entrepreneurs at JSCB "Kapitalbank"

PROCEDURE

for the provision of e-commerce services using cards of international payment systems via the Internet

I. SUPPLEMENTARY TERMS AND DEFINITIONS:

1.1. The following terms and definitions are used in this Procedure:

Authorization is the procedure for requesting and subsequent receipt by a merchant from IPS of permission to conduct an operation using the Card on the Internet site. The confirmation contains a unique code that identifies each specific transaction. The presence of the code in the response received by the merchant from the IPS services is permission to carry out a transaction using the Card.

ASP is a specialized automated software package for processing IPS operations, incl. for payment for goods (work, services) via the Internet installed at the Bank.

Internet platform - an Internet resource of a merchant or its partners, which includes a Website on the Internet that allows the merchant to accept and service orders for the purchase of goods (works, services) via the Internet.

Card – a bank payment card issued by the Issuer to its Holder (the owner of the international card account) under the auspices of the IPS.

Transaction is a non-cash transaction in foreign currency performed by the Holder (the owner of the International Card account) using the Card, with mandatory Authorization.

IPS is a leading international payment system with which the Bank has an agreement to provide Services.

A website is a collection of information, the method of its presentation and technical means, usually united by one topic and/or purpose, which allows a user connected to the Internet and having the appropriate technical means to access this information.

Standards – international standards, incl. approved by the IPS in terms of security (3DSecure, Verified by Visa, Master Card Secure Code, UCAF, Secure Pay, BC Card/Smartro).

Rules – guidelines for the provision of Merchant Services, which are an integral part of this Procedure.

Services – e-commerce services for IPS cards, provided in accordance with the Standards.

Acquirer is a financial institution that is a member of the IPS and provides settlements with merchants for transactions made using Cards.

Issuer is a financial institution that is a member of the International Payment System and issues Cards.

PCI DSS is a payment system security standard that is mandatory for the use of merchants.

1.2. Other terms and definitions used in this Procedure have the same meaning as in the Agreement.

II. GENERAL PROVISIONS

2.1. This Procedure becomes binding for the Parties (enters into force) on the basis of the Application for the provision of e-commerce services using cards of international payment systems via the Internet (hereinafter referred to as the "Application") signed by the Client personally (in paper form) or with an electronic digital signature (in electronic form in the IBC system) and regulates the relationship between the Bank and the Client in connection with the Client's sale of goods (work, services) on the Site or Internet platform with the acceptance of payment through the

use of the Card and the Bank’s organization of such Transactions using the APC for transferring funds to the Client’s accounts.

2.2. This Procedure, the Agreement, the Bank's Tariffs, as well as the Application, together constitute the Contract for the provision of e-commerce services using cards of international payment systems via the Internet VISA (hereinafter referred to as the “Contract”).

III. RIGHTS AND OBLIGATIONS OF THE BANK

3.1. The Bank is obliged:

3.1.1. to provide the Client with access to the ASP for carrying out transactions to pay for goods (works, services) on the Site or Internet platform using Cards;

3.1.2. to organize using the ASP specified in clause 3.1.1 of this Procedure, conducting Transactions carried out using Cards on the Site or Internet platform around the clock (24/7);

3.1.3. to organize the receipt from the Client and processing of authorized Transactions carried out by legitimate Card holders;

3.1.4. to transfer funds paid through Cards to the merchant's current account in accordance with the Bank's Tariffs, to the Client's current account within 5 banking days from the date of processing by the Bank of authorized Transactions issued by the IPS, with the exception of cases under clauses 3.2.7. – 3.2.8 And 3.2.9 this Procedure;

3.1.5. to keep banking and commercial secrets of merchants and Cardholders that have become known to the Bank as a result of fulfilling the terms of the Agreement;

3.1.6. to ensure the safety of transactions for paying for goods (works, services) with a Card on the Site or Internet platform.

3.2. The Bank has the right:

3.2.1. without additional orders (without acceptance) the merchant can write off the merchant's account with the Bank, issue payment requests (without acceptance) to other banks, funds for payment of the Commission in the amount provided for in the Bank's Tariff, as well as other commissions and charges (such as “Chargeback” and “Representation”, “Pre-Compliance”, “Pre-Arbitration”), which were received from IPS for this TSP;

3.2.2. Unilaterally terminate the Authorization of Transactions if the Client violates in accordance with Appendix 2 to this Procedure, as well as the obligations specified in the paragraphs and subparagraphs of Section 4 of this Procedure;

3.2.3. to send the Client a corresponding written notice within 2 (two) business days about the termination of Authorization of Transactions;

3.2.4. to conduct jointly with IPS and/or the Client/unilateral scheduled/unscheduled audit of the Client to identify fraudulent transactions with Cards, provision by the Client to buyers of goods (works, services) not agreed with the Bank and dummy Sites or Internet platforms;

3.2.6. immediately to block all Authorizations if it is established that the goods (works, services) sold on the Site or Internet platform do not correspond to the declared activities, and/or are on the list of prohibited goods in accordance with Annex 4 to this Procedure and/or the INTERNET SITE/MARKET-PLACE engages in illegal activities, including cash withdrawal and/or money laundering;

3.2.7. not to reimburse the Client’s funds in the event of disputes if the Bank has received a “Fraud Report” (fraud report) or “Chargeback” / “Finance Dispute” (rejection of the Transaction) / “presentment” (repeated refusal of the Transaction) for completed Transactions before clarification of all circumstances, which, according to the rules of the Ministry of Railways, can last from one to four months;

3.2.8. to suspend the crediting (freezing) of funds to the Client’s account until the suspicious Transactions that are included in the Fraud Guard or Visa Fraud Monitoring Program are fully verified by sending a request to the Issuer;

3.2.9. to return funds to the issuing banks if suspicious activity is detected by the IPS in the Client's Transactions and a case is opened to protect the brand, or if the threshold limit is exceeded under the program for monitoring suspicious IPS Transactions;

3.2.10. to reserve the right to carry out Authorizations from Cards that do not support “3D Secure” Authorizations;

3.2.11. Unilaterally to suspend the Contract and refuse to carry out transactions with funds in the event that:

- The Client has provided deliberately unreliable documents or has not provided documents requested by the Bank in accordance with the law on the identification of the Client, on the sources of origin of the Client’s funds and (or) other property;

- the Bank has reasonable suspicions that the use of the Contract by the Client and/or the Beneficial Owner is carried out for the purpose of legalizing proceeds from crime and financing terrorism;

- the Bank has information about the Client’s participation or suspicion of participation in terrorist or other criminal activities, obtained in accordance with the current legislation of the Republic of Uzbekistan;

- Seizure of the Client’s funds located on the account, or suspension of operations on the account in cases provided for by the legislation of the Republic of Uzbekistan;

3.2.12. in the manner established by the legislation of the Republic of Uzbekistan and local acts of JSCB “Kapitalbank”, without the Client’s consent, freeze and/or suspend transactions with funds or other property (except for transactions for crediting funds) in cases where, in accordance with current legislation, persons are subject to to the List of persons. In case of suspension of the operation and (or) freezing of funds and other property, funds will not be debited from the Client’s accounts;

3.2.13. to suspend the provision of the Service if there is no communication with the Ministry of Railways.

3.3. The parties may have other rights and obligations provided for by the legislation of the Republic of Uzbekistan and the Agreement.

IV. RIGHTS AND OBLIGATIONS OF THE CLIENT

4.1. The client undertakes:

4.1.1. comply with the Rules specified in Appendix 2 to this Procedure;

4.1.2. ensure that the Internet site or SITE complies with the IPS PCI DSS security standard;

4.1.3. Accept payment for goods (work, services) via Cards at prices not exceeding the price for these goods (work, services) when paid in cash;

4.1.4. In case of refusal by the Holder (owner of the international card account) of the goods (works, services), provide a refund in accordance with the Rules, and the refund can be made in the form of:

- Cancellation transactions – electronically through the personal merchant page on the special website of the Bank and/or IPS before transferring the collected package of Transactions;

- Refund transactions – electronically or in the form of a “Request for Refund Form” in accordance with Appendix 3 to this Procedure, including if it is impossible to complete a Cancellation Transaction;

4.1.5. to post on the Website information related to ensuring the confidentiality of customer data and ensuring the security of payments in accordance with sections 4, 5 of Appendix 2 to this Procedure, as well as sections regulating security issues and the procedure for combating fraud on the Bank’s Website;

4.1.6. to store information on transactions using Cards (registers, customer receipts for goods (works, services), orders to debit the Card, etc.) and transaction reports for at least 18 months from the date of the Transaction, and transfer them to the Bank upon request;

4.1.7.to coordinate with the Bank the design of the payment page of the Site or Internet platform(s), including electronic versions of advertising stickers with the IPS logo specified in Appendix 1 to this Procedure;

4.1.8. It is mandatory to provide the Bank with the following information:

- on the list of goods (work, services) provided by the Site or Internet platform(s) to customers, indicating the min/average/max price of each product (work, service), postal service receipts for sending the goods (work, services);

- About the domain name of the Site or Internet platform(s) and any changes thereto;

- Information about the IP addresses from which the Transaction was carried out, the Site or Internet platform(s) and any changes thereto;

4.1.9. Not to sell goods (work, services) prohibited for sale/provision according to the legislation of the Republic of Uzbekistan. The list of prohibited goods (works, services) is given in Appendix 4 to this Procedure;

4.1.10. provide the Bank and/or IPSwith permanent access to electronic journals and/or databases for recording transactions of each Site or Internet platform;

4.1.11. and the period established by the Bank, provide the Bank with a report on transactions that aroused suspicion of fraud with Cards and/or provision of goods (works, services) to merchants not agreed with the Bank;

4.1.12. regularly check the Site or Internet platform for viruses and vulnerabilities, malware, adware and Trojans, due to which compromise may occur (access by unauthorized persons to customer data and their Cards as a result of illegal actions);

4.1.13. immediately inform the Bank in writing about all changes related to payment details, the nature of the work provided, services and goods sold, changes in other documents and other information about the TSP previously provided to the Bank;

4.1.14. Keep banking and commercial secrets of the Bank and Cardholders that have become known to the merchant as a result of fulfilling the terms of the Agreement;

4.1.15. Provide the completed Form on the activities of the organization given in Appendix 5 to this Procedure.

4.2. The client has the right:

4.2.1. to require the Bank to timely credit the amounts in accordance with clause 3.1.4 (except for cases under clauses 3.2.7 - 3.2.8 and 3.2.9 of this Procedure) of transactions for payment for goods (work, services) made using Cards on the Site or Internet platform;

4.2.2. to refer to the possibility of servicing Cards in your own advertising materials, having previously agreed in writing with the Bank, produce advertising products with IPS trademarks.

4.3. The parties may have other rights and obligations provided for by the legislation of the Republic of Uzbekistan and the Agreement.

V. FINANCIAL TERMS

5.1. Mutual settlements between the Bank and the Client are made in US dollars, in accordance with the legislation of the Republic of Uzbekistan, in the manner and on the terms determined by the Contract.

5.2. The fact that the Client has credited/transferred funds based on the processed Transaction Authorization does not constitute an unconditional recognition by the Bank of the validity of the transaction carried out by the Client.

5.3. The Client does not have the right to split the cost of one purchase (work, service) with two or more Transaction Authorizations, or accept alternative payment for part of the cost of one purchase (work, service) by other means of payment.

5.4. For making payments for transactions for payment of goods (work, services) on the Site or Internet platform using Cards, costs or commissions of the Client's IPS service providers are charged in the specified amount in the Bank's Tariff each time from the amount of compensation.

VI. RESPONSIBILITY OF THE PARTIES

6.1. The parties are responsible for failure to fulfill or improper fulfillment of their obligations under the Contract in accordance with the current legislation of the Republic of Uzbekistan, the Agreement and this Procedure.

6.2. In the event of failure to fulfill or improper fulfillment of obligations under the Contract by one of the Parties, the other Party has the right to demand from the guilty Party the fulfillment of its obligations, as well as compensation for losses caused to it.

6.3. If the Bank violates the established clause 3.1.4 of this Procedure for the deadline for transferring funds, the Bank undertakes to pay the Client a penalty in the amount of 0.1% (Zero point one percent) of the amount to be transferred for each day of delay, but not more than 50% (Fifty percent) of the amount not transferred on time.

6.4. If one of or all of the facts specified in clause 3.2.6 of this Procedure is confirmed, the Client shall pay the Bank a fine in the amount of 5% of the amount of non-conforming goods (work, services).

6.5. The Client is responsible for the actions of its employees related to violation of the terms of the Contract, including its annexes, if they resulted in non-fulfillment or improper fulfillment of the Client's obligations under the Agreement.

6.6. The Client bears full and unconditional responsibility for the compromise of client data and their CARDS caused by hacker attacks on the Site and Internet platform(s), including due to failure to comply with clauses 4.1.2, 4.1.5, 4.1.10 and 4.1.11 of this Order and for incorrect execution or any Transaction made in violation of the IPS rules. In this case, the Bank unconditionally debits funds from the Client's account in the amount of the penalties applied by IPSagainst the Bank.

6.7. The BANK is not responsible for:

- For possible losses of the Client associated with the termination of Authorization of Transactions in the cases provided for in clause 3.2.3 of this Procedure;

- For incorrect execution or any Transaction made in violation of the IPS rules;

- For Transactions on compromised Cards, including if the fact is established or proven that the Transactions were carried out in accordance with the IPS standards;

- if the fulfillment of the Bank's obligations under the Contract depends on certain actions of third parties and/or the IPS Service Provider, or non-fulfillment or untimely fulfillment is due to the fact that third parties and/or the Service Provider cannot or refuse to take the necessary actions or perform them in violation of the established order.

VII. FINAL TERMS

7.1. The Contract comes into force from the moment the Client submits the Application and is valid until the parties fully fulfill their obligations.

7.2. Upon termination of the Contract, commissions paid to the Bank in accordance with the Bank's Tariff are not refundable to the Client.

7.3. Disputes related to the Contract are resolved by the parties through negotiations between themselves. If it is impossible to resolve disputes through negotiations, disputes are resolved in the manner specified in the Contract.

7.4. Relations between the Bank and the Client not provided for by this Procedure are governed by the current legislation of the Republic of Uzbekistan and the Agreement.

7.5. The Parties agree that the source of legal regulation of the relations of the Parties under the Contract is the Contract itself, the Current legislation, Rules, Standards and recommendations of the IPS, if they do not contradict the legislation of the Republic of Uzbekistan. Any terms and conditions of the Contract that contradict the provisions of the Rules (both known at the time of conclusion of the Contract and developed in the future) must be brought into compliance with the Rules.

Annex No. 1
To the Procedure for the provision of e-commerce services using cards of international payment systems via the Internet

List of
Websites/online platforms of trade and service enterprises and international payment systems whose cards are accepted for payment

Name of the Client's INTERNET SITE/MARKET-PLACE with address and telephone number	_____ _____ _____	
NAME OF THE INTERNATIONAL PAYMENT SYSTEM whose cards are accepted for payment (make a note of the system you plan to work with)	☐ Visa ☐ MasterCard ☐ China UnionPay	☐ AMEX ☐ JCB ☐ BC Card / Smartro
Official SITE / MARKET PLACE OF TSP	_____ _____ _____	

SIGNATURES OF THE PARTIES

From the Bank:

Manager:

_____
Full name:

_____
signature

Chief Accountant

_____
Full name:

_____
signature

(seal)

From the Client:

Supervisor:

_____
Full name:

_____
signature

Chief Accountant

_____
Full name:

_____
signature

(seal)

Annex No. 2

to the Procedure for the provision of e-commerce services using

cards of international payment systems via the Internet

RULES

For the provision of e-commerce services using cards of international payment systems via the Internet

1. The procedure for interaction under the CONTRACT for the provision of e-commerce services using IPS cards.

1.1. Information about working in the IPS SERVICE PROVIDER system is located at: _____.

1.2. The BANK takes the necessary actions to register the INTERNET MARKET PLACE in the specialized ASP of the BANK using the specified details.

1.3. The BUYER connects to the INTERNET SITE/MARKET-PLACE via the Internet, forms an order and transfers it for further processing to the specialized hardware and software complex of the INTERNET SITE/MARKET-PLACES.

1.4. The INTERNET SITE/MARKET-PLACE processes the order through the SERVICE PROVIDER's ASP and transfers detail and TRANSACTION parameters to the IPS SERVICE PROVIDER's ASP, depending on the requirements of the IPS SERVICE PROVIDER.

1.5. The BUYER selects a payment scheme (3D-Secure, Verified by Visa, MasterCard SecureCode, UCAF, SecurePay, BC Card/Smartro) and, if necessary, transfers information about the parameters of his CARD to the ASP of the IPS SERVICE PROVIDER, including CVC2 or CVV2 values, expiration date card actions, personal data, which at the same time confirms consent to pay for the order.

1.6. The IPS SERVICE PROVIDER checks the correctness of the format of the entered parameters of the BUYER's card and carries out additional authentication procedures for the BUYER, depending on the supported payment scheme (3D-Secure, Verified by Visa, MasterCard SecureCode, UCAF, SecurePay, BC Card/Smartro).

1.7. If the received request complies with the established standards, the IPS SERVICE PROVIDER submits a request for AUTHORIZATION of the transaction to the BANK.

1.8. The BANK verifies the right of the SITE/MARKET PLACE to conduct the operation in accordance with the registration.

1.9. The BANK carries out AUTHORIZATION OF TRANSACTIONS in the manner established by the relevant IPS.

1.10. When the BANK receives a negative result of the TRANSACTION AUTHORIZATION, the BANK sends a notification of refusal to the ASP of the IPS SERVICE PROVIDER, which, in turn, transmits this information to the INTERNET SITE/MARKET-PLACE AND THE BUYER, indicating the reasons for the refusal.

1.11. If the TRANSACTION AUTHORIZATION result is positive, the BANK transmits confirmation of the positive result to the IPS SERVICE PROVIDER's ASP.

1.12. The ASP of the IPS SERVICE PROVIDER simultaneously transmits confirmation of the positive result of the AUTHORIZATION operation being carried out to the INTERNET SITE/MARKET-PLACE and the BUYER.

1.13. After receiving confirmation of a positive result of the AUTHORIZATION operation, the INTERNET SITE/MARKET-PLACE provides a service (carries out work, releases goods) to the BUYER.

1.14. In accordance with the CONTRACT, the BANK transfers funds to the merchant's current account with the Bank.

1.15. The transfer of funds to the merchant is carried out after the BANK processes the transferred collection package of AUTHORIZED TRANSACTIONS within the period specified in clause 3.1.4 of the CONTRACT.

2. Registration of return or cancellation TRANSACTIONS.

2.1. Registration of return or cancellation TRANSACTIONS in standard cases is completed electronically through the personal page of the TSP or by submitting an application in the form of ANNEX 3 to the CONTRACT.

3. Processing operations in non-standard situations

3.1. If, for technical or other reasons (for example, an error by merchant employees), it is not possible to complete and process the transaction using standard means in accordance with the procedure set out in the Contract, the merchant has the right to contact the BANK with a request to process such a transaction (perform a payment transaction goods (work, services), return, cancellation of payment or cancellation of return) using the technical means of the BANK.

3.2. To process a payment transaction, cancel a payment or cancel a previously made refund, the merchant sends an application to the Bank in the form of Appendix 3 to the CONTRACT, and also attaches all checks, electronic records and other documents available to the merchant that justify the need to process such a transaction. The application must be signed by persons authorized to sign in accordance with the card with sample signatures and seal imprints, and sealed with the TSP seal imprint.

3.3. Based on the results of consideration of the application and attached documents, the BANK has the right to process the transaction specified in the application or refuse processing without explanation; Moreover, the fact of crediting/debiting funds based on the results of processing such a transaction does not constitute the BANK’s unconditional recognition of the validity of this transaction.

4. Payment security

4.1. Payment security is ensured using the BANK's ASP and the IPS SERVICE PROVIDER's ASP, which operates on the basis of modern protocols and technologies developed by the IPS (3DSecure, UCAF, SecureCode).

4.2. In the system of the IPS SERVICE PROVIDER, the security of the BUYER's confidential data is ensured using the SSL protocol.

4.3. Further transfer of information is carried out over closed data networks certified IPS for the delivery of confidential financial information.

4.4. Processing of the received confidential data of the BUYER (CARD details, registration data, etc.) is carried out in the processing center.

5. Security of transmitted information

The security of transmitted information is ensured using modern Internet security protocols (SSL/TLS).

6. OPERATION SCHEME according to the 3D-SECURE security protocol

When using the 3D-SECURE security protocol, there are four parties involved:

Merchants must be enrolled in the service under the Verified by Visa or MasterCard SecureCode program and display the “Verified by Visa” and “MasterCard SecureCode” brands on their websites.

ISSUERS must use an Access Control Server (ACS Server) to authenticate the customer's identity during the transaction process, as well as manage electronically signed receipts.

CARD HOLDERS must be connected to 3D-Secure. The cardholder must enter a password and other security information during the authentication process.

Directory Server. IPS, implementers of 3D-Secure, use a central Catalog Server, which acts as an interaction domain for identification information and addresses of ACS servers of issuers participating in services within the Verified by Visa and MasterCard SecureCode programs.

6.1. Authentication of payment participants

The technology for making payments for goods and services on the Internet, supported within the framework of the project, is based on current IPS specifications, such as Visa (Visa 3D-Secure specification, the name of the marketing program is Verified by Visa) and MasterCard (the SPA/UCAF specification, the name of the marketing program– MasterCard SecureCode).

In order to ensure the necessary level of security, prevent fraudulent transactions and financial losses of participants in electronic transactions on the Internet, both specifications are based on the same fundamental principle - mutual authentication of payment participants. This principle is implemented using a three-domain model (see Fig. 1.).

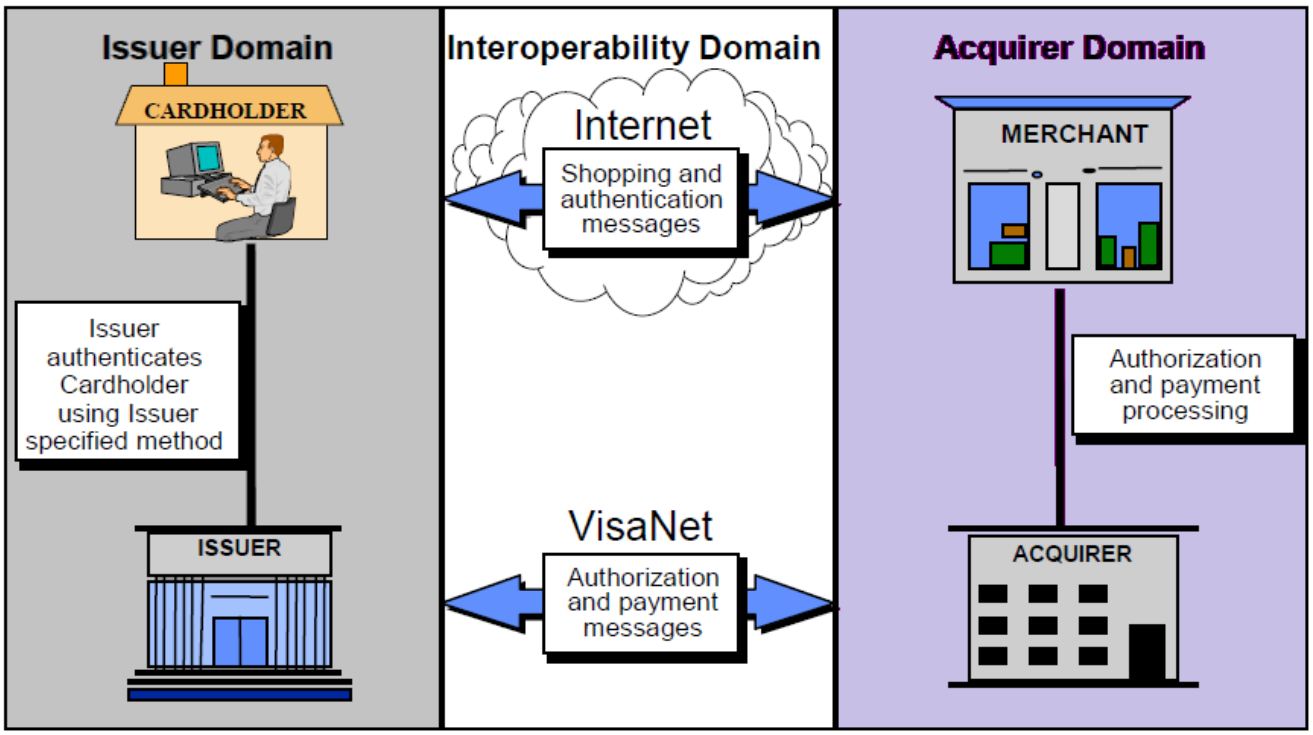

Fig.1. Implementation of authentication using the 3D-Secure protocol using a three-domain model

The purpose of each of the mentioned domains is as follows:

Issuer domain – its purpose is that before performing authorization, i.e. checking the solvency of the card, the issuing bank that issued this card authenticates the buyer - the holder of this card, thereby confirming the authenticity of the buyer's identity. As a result, all responsibility for authentication and for the authenticity of the transaction as a whole falls on the issuing bank.

Acquirer domain - its purpose is that the servicing bank authenticates its merchant outlet based on the rules and methods established by the servicing bank itself (i.e. in this case, all responsibility for authenticating the electronic store falls on the servicing merchant bank).

Interoperability domain - its purpose is to define the rules and procedures for the exchange of information between the ISSUER and ACQUIRER domains, guaranteeing these domains mutual authentication of each other. The specified domain is supported by the IPS itself.

The card holder is in the issuer's domain, and the trade and service enterprise is in the acquirer's domain, which in turn interact with each other through the interaction domain.

Thus, the three domains (3D) model, dividing the process of authentication of transaction participants into separate zones, immediately limits the set of all e-commerce protocols, defining only a certain subset of all possible algorithms for interaction between transaction participants.

It should also be noted that authentication procedures within the ISSUER and ACQUIRER domains are determined by the issuing bank and the acquiring bank, respectively. The IPS defines only the rules of operation in the Interoperability Domain, through which, as noted above, interaction takes place between the client and the point of sale. The network model of three domains clearly defines the responsibility of all participants in the transaction in the process of their authentication (a kind of delegation).

The main and obvious advantage of the model under consideration is that the ISSUER gets the opportunity to authenticate its client in any way convenient for it.

6.2. DESCRIPTION OF PAYMENT TECHNOLOGY

(Using the example of Visa card service)

To make payments using 3D-Secure technology, the CARD HOLDER can be additionally authenticated by linking his international CARD to a mobile phone that is, becoming a participant in the Verified by Visa program.

When making a transaction on the Internet, the store, transferring the main transaction parameters to the centralized resource (the ACQUIRER's payment server), initiates communication between the payment server and the special Visa system in order to check whether the card holder is a participant in the above program.

If the answer is yes, the ISSUER is sent a request to authenticate the CARD HOLDER. This request is sent to the issuer in the form of a string of parameters attached to the web address of the issuing bank's authentication system (the parameters are sent to the buyer's browser). Thus, the buyer is redirected to the authentication system of his ISSUER.

When making a TRANSACTION, an SMS message containing an authentication code is sent to the client's mobile phone, and the client is taken to a special web page protected by the SSL encryption protocol, where he is required to enter the received code (authenticate).

After confirming the identity of the CARD HOLDER, the ISSUER's authentication system generates a special unique digital value that plays the role of a signature certifying this transaction. This signature is transmitted to the payment server and then becomes part of the authorization request that the store (payment server) sends to its ACQUIRER, who, in turn, sends the authorization request to the issuing bank. After checking the signature and making sure that the card is solvent, the ISSUER completes (approves) the transaction. In this way, the ISSUER authenticates the cardholder at the time of payment and notifies the virtual store in real time whether the buyer is indeed the cardholder.

Thanks to this scheme, payments using international Visa cards will be protected from such phenomena as consumer disputes and refusals to complete a transaction.

The individual stages of making a payment on the Internet are illustrated in Fig. 2.

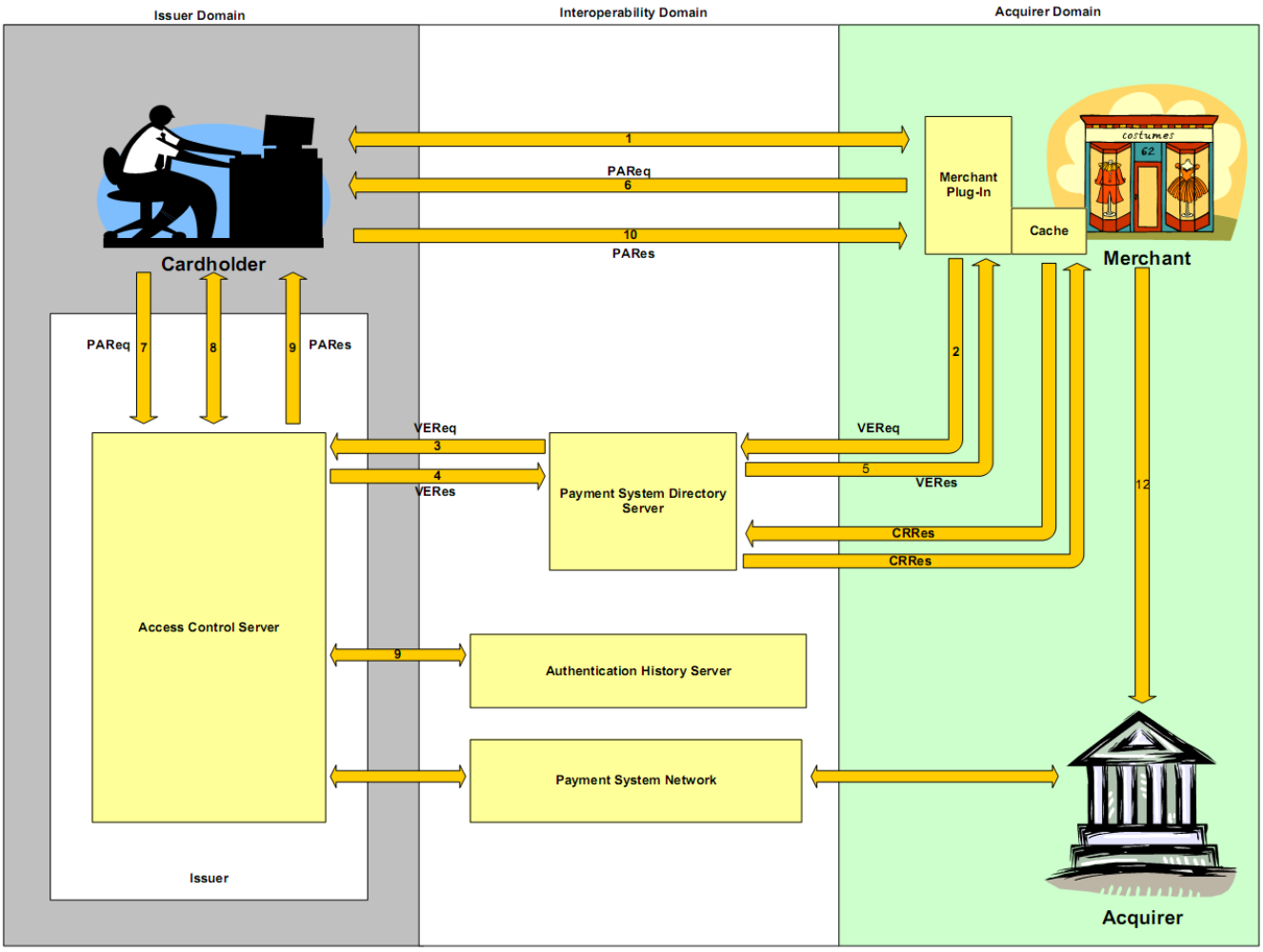

Fig 2. Three-domain scheme for making payments on the Internet, divided into stages:

1. The buyer selects the necessary goods in the electronic online store of the merchant and creates a “basket” of the order.
2. The Merchant Plug-In (MPI) additional software module generates a Verification of Registration Request (VEReq) to the IPS server to determine whether authentication is available for that particular card.
3. If the card number participates in the 3D-Secure service, the Directory Server queries the corresponding ACS Server to determine whether the card is registered with it. (Otherwise, a registration verification response (VeRes) is generated for the MPI module and processing continues from step 5.)

The VeRes response is sent by the Directory Server to the MPI module, notifying the MPI module that authentication is not available for this card. A VeRes response can also be routed from the ACS Server through the Directory Server, as described in steps 4 and 5, if the server determines that the card number is indeed in the participating card range and forwards the request to the appropriate ACS Server.

4. The ACS Server responds to the Directory Server with a VERes response, noting whether authentication is available for the card number.
5. The Directory Server forwards the ACS server's VERes response or its own VERes response to the MPI module if it detects that the card is not in a participating card number range. If the CARD HOLDER is not registered with 3D-Secure or otherwise authentication is not available, the normal authorization request is then provided and the process is completed.
6. The MPI module sends a Payer Authentication Request (PAReq) to the ACS Server using the customer's browser, providing the data necessary to attempt authentication of the CARDHOLDER.
7. The ACS Server receives the PAReq request.
8. The ACS Server authenticates the buyer as matching the card number (including using methods such as password, chip cryptogram or PIN), then formats the Payer Authentication Response (PARes) message with

the appropriate values and puts a digital signature. PARes marks whether the authentication was successful or not.

9. The ACS Server returns the PARes response to the MPI module via the buyer's browser. The ACS Server sends a copy of the PARes response to the Authentication History Server. The Authentication History Server is a component that runs in the Interoperability Domain; archives activities used by ACQUIRERS and ISSUERS for dispute resolution and other purposes.
10. The MPI module receives the PARes response.
11. The MPI module confirms the signature of the PARes response (either by performing the confirmation itself or by passing the message to a separate Validation Server).
12. The merchant exchanges authorization with its ACQUIRER.

Following step 12, the ACQUIRER processes the AUTHORIZATION with the ISSUER through the IPS network and returns the result to the merchant.

6.3. SECURITY QUESTIONS

1. The AUTHORIZATION method used guarantees the Buyer that the payment details of his card (number, expiration date, CVV2/CVC2) will not fall into the hands of fraudsters, since this data is not stored on the trading server of the Internet merchant and, therefore, cannot be stolen from there.
2. The Buyer enters his payment details not on the website of the online store, but directly in the processing center on a secure page of the payment server, therefore, the payment details of the Buyer's CARD will not be available to the merchant staff. This functionality is the implementation of the IPS security requirements for e-commerce TRANSACTIONS.
3. The security of transmitted data is ensured by using the SSL protocol and therefore they cannot be intercepted while being transmitted over communication channels.
4. Information about the CARD details stored for subsequent processing in the processing center database is subject to additional encryption and can only be read by authorized personnel.
5. The security of the exchange of payment information between the online store and the payment server is ensured by the use of the MAC signature mechanism, which eliminates the possibility of distortion of the transmitted information when transmitting it through the Buyer's browser.

7. Requirements for the development of an INTERNET website for a merchant. Policy for returning goods, feedback and customer confirmation of receipt of goods.

7.1 When developing an Internet site, the merchant must take into account the minimum requirements of the bank. Such requirements include the following:

- Develop a product return and feedback policy on the website, indicating the responsible persons.
- Indicate on the website the bank's email address for customer complaints in cases of unauthorized debiting.
- A tool for tracking the delivery of goods.
- Link to apply for a return of goods and funds.
- The merchant must support the ability to request a 3D Secure code from the payer.
- The user (payer) account needs to time out. In case of inactivity for 15 minutes (time for review)
- Consider this possibility: When registering (or at some other "working moment") of the user, add a mobile number to the Visa card details. In order for the site to request an SMS from this mobile number when making a transaction from this card.

7.2 The merchant must store all transaction details on its website for 6 months, and upon the first request of the bank, provide all the necessary information to the service branches or branch. The transaction details must contain the following infrmation.

- Full name of the buyer.
- Product names and quantity.
- Date and time of the transaction.
- From what IP address the authorization and purchase took place.
- The price of the product.
- Buyer's address, email and telephone.
- Order number.
- Attached mobile number with SMS confirmation.

Annex No. 3
to the Procedure for the provision of e-commerce services
using cards of international payment systems via the Internet

APPLICATION FOR OPERATION

_____
(Name of the Client and website/Internet platform)

☐ Expenses Operation[1] ☐ Partial return[2] ☐ Full return[2] ☐ Return[2]

To the Branch Manager _____ JSCB Kapitalbank

I. Instruction for write-off, partial/full cancellation, refund (delete what is unnecessary)

Name of payment system	
Order payment date	
Order payment time	
Order price	
Order number	
Terminal code	
Authorization code	
Last 4 digits of the buyer's card number	
Transaction amount (in numbers and words):	

From the Client:
Supervisor

_____ _____
Signature Full name

Chief Accountant

_____ _____
Signature Full name

(Seal)

«____»_____ 20__year.

[1] Drawn up if there is no technical ability to perform the operation independently or in non-standard cases
[2] Can be issued by the Client in both standard and non-standard cases.

When submitting an application for partial/full cancellation or return of a transaction, the second part is filled in after calculating the total number of transactions to be canceled/refunded.

II. Perform full/partial cancellation of the operation; canceling the return operation, processing the operation, etc. (delete what is unnecessary)

Number of canceled/refunded transactions:	
Total amount in words and figures:	
Collection package number:	
The total amount of the collected package in words and figures:	

«____» _____ 20__ year.

From the Client:
Supervisor

_____ _____
Signature Full name

Chief Accountant

_____ _____
Signature Full name

(Seal) «____» _____ 20__year.

Annex No. 4

to the Procedure for the provision of e-commerce services

using cards of international payment systems via the Internet

LIST OF PROHIBITED GOODS

- Products and/or services of an erotic and pornographic nature.
- Alcohol and alcohol-containing products (including low-alcohol drinks)
- Tobacco and tobacco products.
- License requiring activities, without valid licenses and/or special permits.
- Agency activities without direct contracts with manufacturers/suppliers.
- Medicines and medications, dietary supplements (dietary supplements).
- Historical and cultural values, museum exhibits.
- Narcotic and psychotropic substances prohibited by current legislation.
- Products that are full or partial copies of registered trademark products, without necessarily indicating on the website (as well as on the products themselves) that these are copies.
- Charity, contributions, donations without appropriate licenses (registration).
- Sale of digital goods without agreements with suppliers (distributors) and/or copyright holders.
- All types of gambling (except for officially registered lotteries, in accordance with the law).
- Sales and distribution of products and materials promoting violence, ethnic hatred, terrorism and extremist activities.
- Goods and/or services that contradict the Current legislation or are subject to restrictions or other trade rules.
- Payment systems and/or aggregators of payment instruments for trade and service enterprises, providing payment services in favor of third parties, replenishing one's own "virtual" account with subsequent spending of funds on goods/services of third parties, exchange and/or conversion of credited funds, electronic currencies, as well as withdrawal and/or cash withdrawal of funds from a "virtual" account.

Annex No. 5
to the Procedure for the provision of e-commerce services using cards of international payment systems via the Internet

Merchant application form.
Form about the activities of the organization.

Corporation details.	
Company Name	
Registered address	
Post code and city	
Contact Person name, phone and email.	
Bank account information	
Main Account	
Bank name	
Account number	
Bank branch	
Swift code	
Website details	
Website name	
Type of business	
IP Address	
Customer Support email	
Chargeback notification email..	
How long have you been in business?	
Currently monthly sales volume.	
Current number of monthly transaction.	
How do you receive your customer's order?	Internet _____ (%) Telephone order _____ (%)
SSL certificate, when, where and expire date.	
Technical contact name of web site, phone and email.	
Website content	
What is/ are the product/s or services sold on your website?	
Min / average / max price of goods / services on the site	
Describe the terms of delivery of goods, and the terms of the service.	
Describe the terms of return police or cancel services.	
Do you send an email receipt to the cardholder when the product delivered? Describe for example.	