“Common Republican Processing Center” Joint-Stock Company

“APPROVED”
Deputy General Director for Information Security of UCMG LLC

REGULATIONS FOR CONDUCTING ORGANIZATIONAL AND TECHNICAL VERIFICATION OF COMPLIANCE WITH INFORMATION SECURITY REQUIREMENTS OF THE UZCARD PAYMENT SYSTEM

TASHKENT - 2025

TABLE OF CONTENTS

1. GENERAL PROVISION 4
2. Types of conducting Organizational and Technical Verification of a Partner 4
3. Primary Organizational and Technical Verification of a Partner 4
4. Secondary Organizational and Technical Verification of a Partner 5
5. Organizational and Technical Verification of a Partner based on self-assessment form 6
Appendix 1 8
Appendix 2 10
Appendix 3 12
Appendix 4 13
Appendix 5 14

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

Partner	Payment Service Providers (bank, payment organization, payment agent, and payment sub-agent)
IS	Information Security
OTP	Organizational and Technical Verification of a Partner
ISR	Information Security Requirements outlined in the Rules of the Payment System “UZCARD”
PS «UZCARD»	The payment system “UZCARD” is a system in which the operation and functioning are ensured by the Operator
PIS	The Partner’s Information System is a complex of specialized computer software products, the functioning of which is ensured through information and technological interaction between the Partner and the Operator. It is intended to create an additional service, provide information support, and other services offered by the Partner to its clients.
«SV-Gate»	The Operator’s software is designed for technological interaction between the Partner’s Information System (PIS) and the Payment System “UZCARD”. It enables the utilization of the Operator’s services through the Partner’s IS.
Operator	«Common republican processing center» JSC
Agreement	The agreement concluded between the Operator and the Partner for the temporary paid use of user accounts and software rights for "SV-Gate" through the API (a simple non-exclusive license).
Partner	The bank, payment organization, payment agent, and payment subagent with whom the contract is concluded.
CD	The commercial department of the Operator.
CO	A standing commission for conducting scheduled and unscheduled organizational and technical inspections appointed by order.

1. GENERAL PROVISIONS

1.1. This document establishes the procedure for OTP verification in compliance with the information security requirements of the UZCARD payment system, which is carried out by “CRPC” JSC (hereinafter referred to as the Operator) under the terms set forth in this Regulation, the Information Security Policy (ISR), and the Agreement.

1.2. The purpose of conducting OTP is to assess the readiness of the Partner’s organizational and technical resources in the field of IS in the PIS. The PIS consists of a complex of specialized computer software products (hereinafter referred to as PIS) that are either being connected or already connected to the SV-Gate software.

1.3. The list of documents based on which OTP is conducted includes:

- Law of the Republic of Uzbekistan No. 578 dated 01.11.2019 “On Payments and Payment Systems”;
- Rules of the UZCARD payment system;
- Agreement;

1.4. The participants involved in conducting OTP are:

- Partner;
- CD;
- CO.

2. TYPES OF CONDUCTING OTP

2.1. OTP is conducted based on the agreement concluded between the Operator and the Partner for the registration of a user account and the provision of the right to use the SV-Gate software.

2.2. OTP has 3 (three) types:

2.2.1. Primary OTP – the procedure for conducting is provided in Appendix 3;

2.2.2. Secondary OTP – the procedure for conducting is provided in Appendix 4;

2.2.3. OTP based on self-assessment form – the procedure for conducting is provided in Appendix 5.

3. PRIMARY OTP

3.1. General procedure

Primary OTP is carried out at the initial connection of the Partner's Information System to “SV-Gate” software. It is assumed that the PIS does not have access to the SV-Gate software at the beginning of the OTP. The basis for conducting OTP is the Agreement.

3.2. Preliminary familiarization of the Partner with the ISR and this Regulation

After the Agreement is concluded, the Commercial Department (KD) conducts familiarization of the Partner with the Information Security Policy (TIB) and this document by providing internet links to the current Regulation and TIB. After reviewing the aforementioned documents, the Partner initiates the process of preparing the required data package as specified in the TIB.

3.3. Planning of OTP

During the planning stage, the CO carries out the process of coordinating OTP with the Partner. Primary OTP is conducted with the presence of CO representatives visiting the Partner's premises. If it is not possible for CO representatives to visit the Partner's premises due to operational reasons, the format of conducting OTP may be changed to an online format with prior agreement between CO and the Partner.

3.4. Conducting OTP

At this stage, the Partner provides data to the CO, based on which the main phase of OTP is conducted. During this phase, the provided data is analyzed for compliance with the ISR. A detailed description of conducting OTP is provided in the *Appendix 1*.

3.5. Final report and compliance assessment

After conducting OTP, the CO initiates the preparation of the final report. In case of identification of non-conformities subject to prompt elimination, the process of interaction with the Partner is initiated in order to eliminate them in a timely manner. Based on the collected data, the CO finalizes the report and provides an assessment of the readiness of the PIS in accordance with the ISR:

a) If the PIS complies with the ISR, the activation of the Partner's user account is approved;
b) If the PIS partially complies with the ISR, the activation of the Partner's user account is approved with a conditional period of up to 90 calendar days;
c) If the PIS does not comply with the ISR, the activation of the Partner's user account is not approved.

In case the PIS does not comply with the ISR, the activation of the user account for accessing the SV-Gate software is not carried out. The Commercial Department (CD) sends a report to the Partner and a re-assessment is scheduled. The re-assessment of the PIS is conducted no earlier than 90 calendar days from the date of issuing the negative report, unless an earlier timeframe is mutually agreed upon. If the Partner fails to provide evidence of addressing the noncompliances, the CD initiates the contract termination procedure.

4. SECONDARY OTP

4.1. General procedure

Secondary OTP is applied to Partners who already have access to the SV-Gate software. The secondary OTP is conducted according to the internal "Plan for conducting OTP for Partners" developed by the CO and the Commercial Department (CD).

4.2. Partner notification

The secondary OTP for Partners is conducted based on a notification letter about the upcoming OTP. After the internal "Plan for conducting OTP for Partners" is prepared jointly by the CO and CD, the process of preparing and sending the notification letter to the Partner about the upcoming OTP begins 30 (thirty) calendar days prior to the start of the secondary OTP. Upon receiving the letter, the Partner confirms receipt within 3 (three) working days and initiates preparations for the secondary OTP.

4.3. Planning of Secondary OTP

The CO initiates the process of coordinating the secondary OTP with the Partner, following the process described in Appendix 1. Secondary OTP can be conducted online or with the visit of the CO's representatives to the Partner's territory with the prior agreement of the CO and the Partner.

4.4. Conducting Secondary OTP

On this stage, the Partner provides data to the CO, based on which the main phase of OTP is conducted, comments identified during the previous OTP are discussed, and the submitted data is analyzed for compliance with the ISR. A detailed description of the OTP process is provided in the *Appendix 1*.

4.5. Final report and compliance assessment

After conducting the OTP, the CO initiates the preparation of the final report. In case of identification of non-conformities subject to prompt elimination, the process of interaction with the Partner is initiated in order to eliminate them in a timely manner. Based on the collected data, the CO finalizes the report and provides an assessment of the readiness of the PIS for compliance with the ISR:

a) **If the PIS complies with the ISR, the activation of the Partner's user account is approved;**
b) **If the PIS partially complies with the ISR, the activation of the Partner's user account is approved with a conditional period of up to 90 calendar days;**
c) **If the PIS does not comply with the ISR, the activation of the Partner's user account is not approved.**

In case the PIS does not comply with the ISR, the CD sends the Partner a report and a cover letter to the report, and the account to the SV-Gate software is restricted or disabled until the identified discrepancies are eliminated. The Partner eliminates the identified nonconformities and notifies the CO about the work done and provides materials confirming the elimination of nonconformities. If the Partner fails to provide evidence of elimination of nonconformities within 90 (ninety) calendar days, the CD initiates the procedure of contract termination.

5. OTP BASED ON SELF-ASSESSMENT FORM

5.1.General procedure

The completion of the ISR Self-Assessment Form (hereinafter referred to as the "Form") is conducted in accordance with the internal "Partner OTP Plan". The decision to conduct the assessment by filling in the Form is made solely by the CO in the course of the preparation of the internal "Partners' OTP Plan". The Form is filled in a special electronic system. Access to the system is strictly through a secure VPN channel.

5.2. Partner notification

The CD starts the process of preparing and sending the notification letter to the Partner about the forthcoming OTP. The CO shall provide the Partner's responsible employee with credentials for access to the system of filling in the Form.

After receiving the letter, the Partner confirms receipt within 3 (three) working days and begins the process of filling out the Form. If there are any questions, the Partner can contact the CO for clarification and additional information. Upon completion of the Form, the CO verifies that it was completed correctly and further analyzes the submitted data for ISR compliance.

5.3. Final report and compliance assessment

After conducting the OTP, the CO initiates the preparation of the final report. In case any non-compliances are identified, a process of interaction with the Partner takes place to address the identified non-compliances. Based on the collected data, the CO finalizes the report and provides an assessment of the readiness of the PIS for compliance with the ISR:

a) **И If the PIS complies with the ISR, the activation of the Partner's user account is approved;**

b) If the PIS partially complies with the ISR, the activation of the Partner's user account is approved with a conditional period of up to 90 calendar days;

c) If the PIS does not comply with the ISR, the activation of the Partner's user account is not approved.

In case the PIS does not comply with the ISR, the CD sends the Partner a report and a cover letter to the report, and the account to the SV-Gate software is restricted or disabled until the identified discrepancies are eliminated. The Partner eliminates the identified nonconformities and notifies the CO about the work done and provides materials confirming the elimination of nonconformities. If the Partner fails to provide evidence of elimination of nonconformities within 90 (ninety) calendar days, the CD initiates the procedure of contract termination.

6. CONCLUDING PROVISIONS

6.1. This regulation comes into effect on the date specified in the corresponding order regarding the document's implementation.

6.2. The individuals responsible for the implementation of this regulation are the employees of the Information Security Department, as stated in the aforementioned order.

These Regulations may be revised in case of changes in regulatory and legal acts of the Republic of Uzbekistan, regulatory acts and prescriptions, regulatory and supervisory bodies, contractual terms of the Company with third-party organizations, results of information security audit.

Appendix 1
"Regulations for conducting organizational and technical verification for compliance with the requirements of information security of the UZCARD payment system"

DETAILED PROCESS OF CONDUCTING OTP

1. Preliminary collection of information for OTP preparation.

To conduct the preliminary information collection, the CO sends the Partner the document "Initial Data" provided in Appendix 2 for completion by the Partner.

When filling out the document "Initial Data" from the Partner's side, the following information is provided:

- Information about the Partner.
- PIS software tools.
- PIS network technical tools.
- Payment card data storage locations in the PIS segment.
- Organizational and regulatory documents in the field of Partner's information security.

2. Definition of the scope of OTP

At this stage, the scope of OTP is determined, i.e., the scope of application of the ISR document is identified. The main scope of OTP is the segment of PIS's operations that interact with the SVGate software. The segment of PIS's operations includes the following:

- Regulatory documents defining the work of information security.
- PIS application server - a virtual server where payment card data received from the SV-Gate software is processed. The number of application servers can be more than one virtual server, considering the deployment structure for fault tolerance and load balancing.
- PIS DBMS Server - a virtual server where the PIS database is configured and provides storage and processing of payment card data received from the SV-Gate software. The number of DBMS servers can be more than one virtual server, considering the deployment structure for fault tolerance and load balancing.
- Load Balancer Server - a virtual server that serves the role of load distribution and/or acts as a separate server interacting with the SV-Gate software and the PIS server.
- Inter-network firewalls - interacting with the SV-Gate software and controlling the PIS segment at the network level. Intrusion detection and prevention modules for the PIS segment, which are part of the inter-network firewalls, are also included in the scope of OTP. Information security tools that interact with the PIS segment, such as:
  - Security Information and Event Management (SIEM) system;
  - Privileged Access Management (PAM) system;
  - Antivirus protection system;
  - Data Loss Prevention (DLP) system;
  - Server monitoring and status tracking system for the ISP (Monitoring and Management Service);
- Payment application in the form of a mobile application for iOS or Android, Web portal for the payment application, PIS service in the form of an API.

3. Determination of the OTP implementation method

The next stage involves the agreement on the method of conducting OTP. By default, OTP is conducted on the Partner's premises.

In terms of conducting OTP during site visits, the following are coordinated:

- Date and time of the meeting.
- Approximate duration of the OTP, depending on the scope of the OTP.
- Venue location, the address of the Partner's site;

In cases where it is impossible for the CO to visit the Partner's premises for operational reasons, with the agreement of both parties, the OTP is conducted via remote session using pre-agreed software for online meetings.

4.Preparation on the Partner's side

The Partner begins preparations for the OTP. During the preparation phase, the Partner is required to:

•Prepare for familiarization the regulatory and managerial documents that define the work of information security, journals of document familiarization, and requests for granting access to system administrators and developers to the PIS segment;

•Prepare the logical network topology of the PIS segment for presentation.

•Prepare the data from the firewalls in the inspection area, either in the form of screenshots or through a web platform.

•Prepare the information about the security tools used for the PIS segment, either in the form of screenshots or through a web platform.

•Prepare the cover pages of the latest reports on external and internal vulnerability scanning of the tested segment, as well as the latest penetration testing report for the PIS segment.

•Prepare samples from test and production PIS DBMS databases, where UZCARD payment card data is stored in the form of screenshots or via web platform.

5. Organization of OTP and Compliance Analysis with Information Security Requirements

At this stage, the OTP and compliance analysis with the requirements of ISR are conducted based on the data provided by the responsible employees of the Partner. The results of the conformity analysis are recorded in the CO's dedicated electronic system for conducting the OTP. All requirements listed in the ISR are checked, each requirement is evaluated and an assessment is made:

"Meets" - if the requirement is fully met;

"Partially meets" - if the requirement has not been fully complied with. In such a case, the specific reason why the requirement was determined to be partially met and a recommendation to correct the identified deficiency shall be provided;

"Does not meet" - if the requirement has not been met. In such a case, the specific reason why the requirement was determined not to be met and a recommendation to correct the identified deficiency shall be given;

"Not applicable" - if the requirement is not applicable to the Partner's activities;

6. Conclusion and Formation of Reporting Documentation

After the OTP, based on the provided data, the CO prepares within 3 working days a "Report on the results of the conducted OTP for compliance with UZCARD information security requirements" and gives an assessment of the PIS's readiness for compliance with the ISR.

Appendix 2
"Regulation for
conducting organizational and technical verification for
compliance with the information security requirements of the
UZCARD payment system"

Initial information about the Partner

1. Information about the Partner:

Information about the Partner:	
1. Form of organization	*LLC, JSC, JSCB*
2. Name of the organization	*«Company»*
3. CB license	*№XX from day.month.year (01.01.2024)*
4. PCI DSS certificate	*Current from 01.01.2024 to 01.01.2025*
5. Director / Chairman of the Board	*Full name*
6. Project Manager	*Full name*
7. PIS system administrator	*Full name*
8. Responsible for the IS of the PIS	*Full name*

2. List of software and hardware tools used:

Name	***Description/Purpose***
I. Software tools	
1. Name of PIS	*Application " ", Android, iOS, Web. + application versions*
2. Virtualization system	*VMWare, ESXi, KVM + version*
3. Processing servers (Frontend, Backend)	*Number of servers, role (primary, backup), OS type and version*
4. Database management system (DB)	*Number of servers, role (primary, backup), OS type and version, DBMS version*
5. Antivirus software	*System name and current version Esset, Kaspersky*
6. SIEM system	*System name and current version QRadar, ArcSight, Splunk, Wazuh*
7. PAM system	*System name and current version FudoPAM , SingleConnect, One Identity Safeguard*
8. DLP-system	*System name and current version: SearchInform, Falcongaze., etc.*
9. Web and/ or proxy server, load balancer	*Load Balander, HAPROXY, NGINX, etc.*
10. ntrusion Detection System (Host-based IDS and Network IDS)	*System name and current version WAZUH FIM, Fortigate IPS, etc*
11. WAP (Web Application Protection) or WAF (Web Application Firewall)	*NGINX ModSecurity, FortiWAF, Barracuda WAF, Cloudflare WAF*
II. Technical tools	

1. Network firewall	*FortiGate 200F, PaloAlto PA-3060, Juniper SRX1600*
2. Hardware/Software load balancer	*F5 BIG-IP, Citrix ADC, FortiADC Nginx, HAProxy*
3. DC	*HID Global, ZKTeco, Hikvision*
4. DCMCS	*Hikvision HikCentral, Dahua DSS*

3. List of payment cards data storage locations:

№	*Storage locations*	*Information protection mechanism*	*For what purposes*
1.	*Table in the database that stores UZCARD PCD*	*AES 256, RSA 2048 or no*	*Processing, storage of users' PCD*
2.			

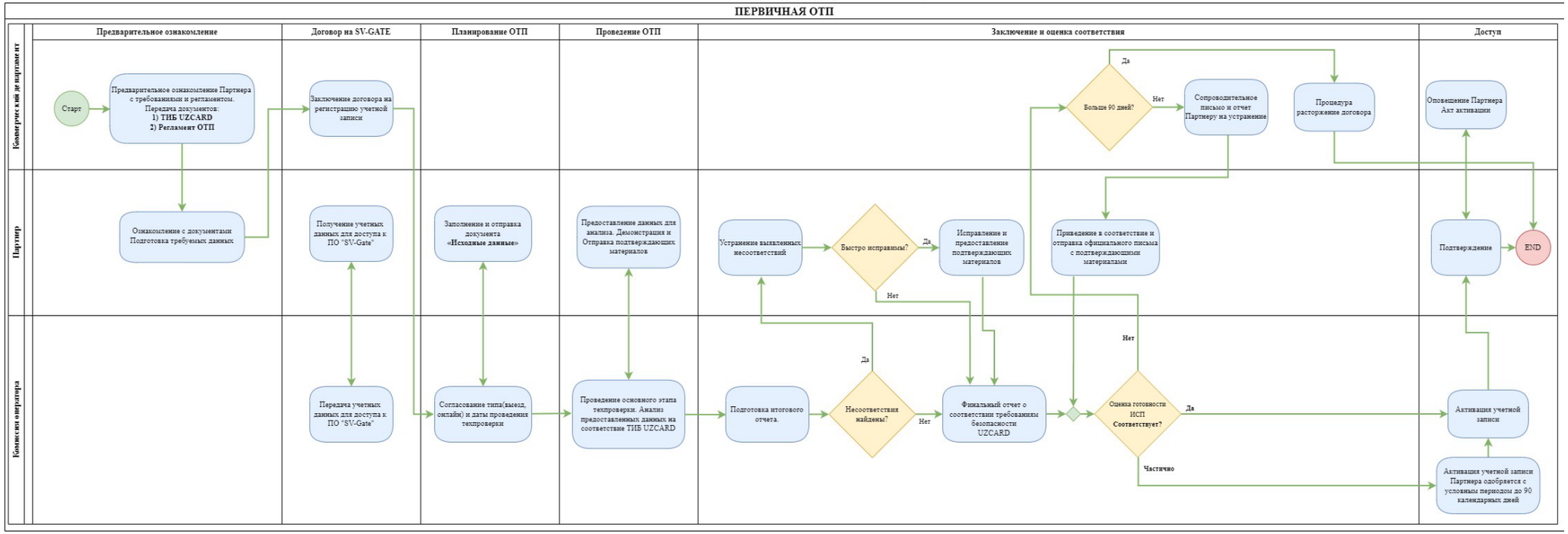
4. List of Partner's regulatory documents in the field of information security:

№	*Name*	*Note*
1.	*EXAMPLE: Information Security Policy of JSC "Company"*	*Approved by the date of 01.01.2024*
2.	*EXAMPLE: IS Risk Assessment and Analysis Methodology*	*Prescribed in the IS Policy*
3.	*EXAMPLE: IS Incident Response Regulations*	*Approved as of 01.01.2024*

Appendix 3

"Regulation for conducting organizational and technical verification for compliance with the information security requirements of the UZCARD payment system"

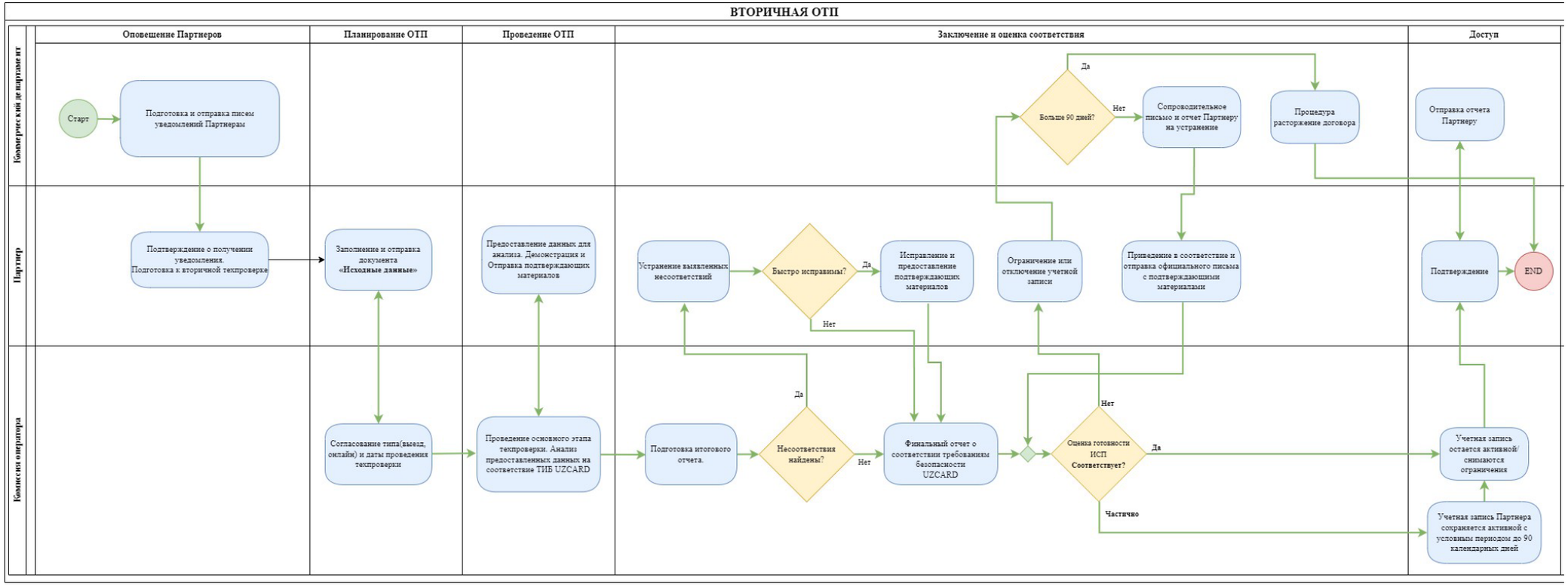
Scheme of Conducting Primary OTP



Appendix 4

"Regulation for conducting organizational and technical verification for compliance with the information security requirements of the UZCARD payment system"

Scheme of conducting Secondary OTP



Appendix 5
"Regulation for conducting organizational and technical verification for compliance with the information security requirements of the UZCARD payment system"

Scheme of conducting OTP through filling the Form

