Акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстан»

Утверждено
решением Правления
АО «НПК»
от «14» февраля 2024 года
(протокол № 3)

Руководство по подключению и взаимодействию с Операционным центром акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан» для взаимодействия с международной платежной системой Visa Int. (адаптационная модель) Рег. № 26

г. Алматы

Содержание

1. Общие положения 4
2. Сервисы и функции операционного центра 5
3. Требования к участникам 6
4. Подключение участника к операционному центру 7
5. Тестирование участника 7
6. Обмен информацией 7
7. Совершение и обработка операций 8
8. Расчетные взаимоотношения между участкниками 8
9. Порядок обеспечения бесперебойности функционирования 9
Приложение 1 10
Приложение 2 11

1. Общие положения

1. Настоящее Руководство по подключению и взаимодействию с Операционным центром акционерного общества «Национальная платежная корпорация Национального Банка Республики Казахстан» для взаимодействия с международной платежной системой Visa Int. (адаптационная модель) (далее – Руководство) описывает порядок подключения и взаимодействия с Операционным центром.

2. Основной задачей документа является определение функциональности, требований, перечня и последовательности мероприятий по подключению банков-участников международных платежных систем к Операционному центру и дальнейшему взаимодействию Операционного центра и банков-участников.

3. Документ предназначен для специалистов процессинговых центров, подразделений информационных технологий, операционных служб, служб безопасности.

4. В руководстве используются следующие понятия:

1) АО «НПК» – акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстан»;

2) Операционный центр (ОЦ) – АО «НПК», в качестве операционного центра международной платежной системы Visa Int. (далее – Visa) обеспечивает от ее имени маршрутизацию, обработку авторизационных, финансовых/нефинансовых сообщений, клиринг и расчеты. ОЦ, в соответствии с заключенными договорами, оказывает банкам-участникам Visa услуги по маршрутизации, обработке сообщений, клирингу и расчетам;

3) участник – банк-участник, подключенный к ОЦ для взаимодействия с ОЦ и другими участниками;

4) МПС – международная платежная система;

5) БИН – банковский идентификационный номер участника;

6) ФАСТИ – финансовая автоматизированная система транспорта информации, предназначенная для защищенного обмена информацией;

7) ЦОД – основной и резервный центр обработки данных ОЦ;

8) внутринациональная операция – операция в национальной валюте по карте участника-эмитента, совершенная в устройстве Казахстанского участника-эквайера, торгово-сервисное предприятие которого надлежащим образом зарегистрировано и осуществляет свою деятельность на территории Республики Казахстан. Операция классифицируется как внутринациональная, если эквайринговый идентификатор участника-эквайера принадлежит участнику-резиденту Республики Казахстан, при этом БИН участника-эмитента, также, принадлежит участнику-резиденту Республики Казахстан;

9) международная операция – операция по карте МПС Казахстанского участника-эмитента, совершенная в устройстве зарубежного эквайера, либо операция по карте МПС зарубежного эмитента, совершенная в устройстве участника - эквайера Республики Казахстан.

5. ОЦ получает авторизационные запросы по внутринациональным операциям от Участников - эквайеров и маршрутизирует их в МПС. МПС направляет авторизационный запрос эмитенту и получив ответ направляет его в

ОЦ. После получения ответа ОЦ обеспечивает маршрутизацию авторизационных ответов до участников - эквайеров.

6. Авторизационные сообщения (запросы и ответы) по картам МПС должны направляться участниками в ОЦ по протоколу МПС.

7. Функционирование ОЦ и участников осуществляется в рамках действующих правил и тарифов МПС.

2. Сервисы и функции ОЦ

8. ОЦ предоставляет участникам перечисленные ниже сервисы.

9. Сервис маршрутизации авторизационных и финансовых / информационных сообщений:

1) участник подключается как напрямую к ОЦ для проведения внутринациональных операций, так и одновременно к МПС для проведения международных операций;

2) ОЦ получает онлайновые авторизационные запросы по внутринациональным операциям от участников-эквайеров и маршрутизирует их в МПС. МПС по собственным процедурам направляет запрос к участнику-эмитенту. Участник-эмитент принимает и обрабатывает авторизационный запрос и посылает ответное сообщение в МПС. МПС направляет ответ участника-эмитента в ОЦ. ОЦ направляет ответ участника-эмитента, полученный от МПС, участнику-эквайеру;

3) маршрутизация авторизационных запросов по внутринациональным операциям в ОЦ выполняется участниками с использованием БИН-таблицы, предоставляемой МПС участникам напрямую;

4) в случае невозможности ОЦ по технической или какой-либо иной причине предоставлять услуги, участники-эквайеры отправляют авторизационные запросы напрямую в МПС. Отправка клиринга, также, должна осуществляться в МПС для внутринациональных операций, авторизационные запросы которых, были отправлены напрямую в МПС.

10. Сервис поддержки авторизационных и финансовых интерфейсов:

- авторизационные и финансовые/информационные сообщения будут направляться Участниками в ОЦ по протоколам МПС.

11. Сервис тестирования, подключаемого участника.

В рамках тестирования выполняется:

1) проверка корректности маршрутизации сообщений - запросов и ответов в формате авторизационных протоколов МПС;

2) проверка корректности настройки программно-аппаратных средств, участвующих в техническом взаимодействии ОЦ и участника.

12. Сервис обмена информацией с участниками (файловый обмен).

Для обмена информации с участниками используется ФАСТИ, предназначенная для организации защищенной транспортной среды обмена данными. ФАСТИ позволяет решать следующие задачи:

1) обеспечение гарантированной доставки информации между участником и ОЦ;

2) защиту от изменения и потери данных по пути от источника к получателю.

3. Требования к участникам

13. Участники должны соответствовать следующим требованиям:

1) иметь сертифицированный МПС процессинговый центр с техническим и программным обеспечением, необходимым для проведения операций по выпуску и/или обслуживанию платежных карт с возможностью прямого подключения к ОЦ;

2) обеспечивать бесперебойность функционирования процессингового центра и аппаратно-программного комплекса, в том числе, обеспечивать функционирование каналов связи до ЦОД ОЦ для обмена информацией;

3) обеспечивать наличие, актуализацию и тестирование процедур восстановления процессингового центра, каналов связи и аппаратно-программного комплекса, задействованных в рамках функционирования и влияющих на бесперебойность работы;

4) обеспечивать сохранение банковской тайны, защиту информации о персональных данных клиентов в соответствии с законодательством Республики Казахстан;

5) обеспечивать соответствие актуальным требованиям стандартов информационной безопасности PCI DSS;

6) иметь квалифицированный персонал для обеспечения бесперебойного и безопасного функционирования системы;

7) пройти процедуры тестирования с ОЦ.

14. Участники, для взаимодействия с ОЦ должны поддерживать форматы авторизационных интерфейсов МПС.

15. Участники должны провести следующие мероприятия для организации телекоммуникационного взаимодействия:

1) организация не менее 2х выделенных, защищенных (основных и резервных) телекоммуникационных каналов связи между участником и ЦОД ОЦ;

2) предоставление адреса шлюза для связи основного и резервного процессинговых центров участника с ОЦ;

3) прохождение процесса тестирования без ошибок и сбоев работе.

16. Организация телекоммуникационных каналов связи является ответственностью участника. Каналы связи между основными и резервными процессинговыми центрами участника к ЦОД ОЦ должны быть реализованы через выделенные каналы связи с пропускной способностью:

- для трафика с максимальной нагрузкой до 10 тр/с - 512 Кбт/с;
- для трафика с нагрузкой в пределах 10-100 тр/с - не менее 1 Мбит/с;
- для трафика с нагрузкой свыше 100 тр/с - 2 Мбит/с.

С возможностью изменения в зависимости от объема транзакций, и обеспечены возможностью шифрования от сетевого оборудования участника до сетевого оборудования ОЦ. Допускается использование существующих каналов связи между ОЦ и участником с учётом текущей утилизации и необходимой пропускной способностью в соответствии с руководством.

4. Подключение участника к ОЦ

17. ОЦ производит следующие действия:

1) присваивает участнику идентификатор в системе и дополнительные регистрационные параметры, необходимые для работы в системе;

2) предоставляет участнику детали коммуникационного подключения к ЦОД ОЦ.

18. Участник производит следующие действия:

1) организовывает и обеспечивает дальнейшую поддержку основного и резервного каналов связи с ЦОД ОЦ;

2) производит настройку программного обеспечения для обработки операций по платежным карточкам по каналам связи с ОЦ.

19. ОЦ совместно с участником выполняет следующие действия:

1) производит тестирование систем участника обеспечивающих взаимодействие с ОЦ;

2) после успешного завершения тестирования ОЦ принимает решение о подключении процессингового центра участника к ОЦ.

20. Любое изменение конфигурации программных и аппаратных средств участника, влияющее на взаимодействие с ОЦ и другими участниками, может потребовать дополнительного тестирования, необходимость которого определяется дополнительно.

5. Тестирование участника, подключаемого к ОЦ

21. При проведении тестирования процессингового центра участника, с целью проверки его технической готовности к взаимодействию с ОЦ, участнику необходимо проверить:

1) готовность тестового комплекса участника для проведения тестирования с ОЦ;

2) корректность настройки программно-аппаратных средств, каналов связи, участвующих в техническом взаимодействии ОЦ и процессингового центра участника;

3) запросы на авторизацию сообщений и отмены авторизованных операций формируются корректно и получаются ожидаемые ответы от эмитента.

22. Участник может дополнительно провести:

1) доработки информационных систем участника, обеспечивающих взаимодействие с ОЦ или своим процессинговым центром;

2) актуализацию внутренних операционных регламентов и иных нормативных документов участника.

6. Обмен информацией

23. Обмен информацией и документацией осуществляется одним из нижеприведенных способов, при этом всю ответственность за конфиденциальность содержимого несет отправитель:

1) ФАСТИ;

2) курьером, с уведомлением о вручении;

3) почтой, заказным письмом с уведомлением о вручении;

4) электронной почтой на адреса, указанные в договоре.

24. Основным способом обмена информацией является система ФАСТИ, предназначенная для организации защищенного обмена информацией.

25. Состав программного обеспечения пользователя.

Для работы системы ФАСТИ на персональном компьютере пользователя необходимо:

1) ключи и регистрационные свидетельства участника, выпущенные Удостоверяющим центром АО «НПК»;

2) ПО «Криптопровайдер Tumar CSP» с соответствующими плагинами (программными компонентами, позволяющими реализовать дополнительные функции) устройств хранения ключевой информации;

3) клиентское приложение «VIDO5».

7. Совершение и обработка операций

26. Маршрутизация авторизационных запросов и финансовых/информационных сообщений осуществляется на основании БИН участников по операциям, совершаемым с использованием платежных карт участников в сети обслуживания других участников.

27. Участник, получив актуализированную информацию по БИН обязуется принять и внести изменения в базу данных своего процессингового центра не позднее следующего рабочего дня с даты их получения.

28. ОЦ полностью приостанавливает и возобновляет маршрутизацию авторизационных запросов и финансовых/информационных сообщений участника по письменному уведомлению Национального Банка Республики Казахстан о прекращении активных операций пользователя в межбанковской системе переводов денег, нарушения условий договора овердрафта, а также на основании других уведомлений Национального Банка Республики Казахстан. ОЦ имеет право принять экстренные меры, вплоть до остановки маршрутизации авторизационных запросов и финансовых/информационных сообщений участника, без предварительного уведомления в случае обнаружения ОЦ инцидентов приведших или имеющих возможность привести к потенциальной угрозе несанкционированного доступа или взлома системы, допущенных по вине участника и/или нарушения информационного взаимодействия.

29. Все диспутные процедуры, урегулирование споров по карточным операциям, участники регулируют с помощью сервисов и действующих правил МПС без участия ОЦ.

8. Расчётные взаимоотношения между участниками

30. Клиринг обработанных через ОЦ внутринациональных операций участников выполняется МПС, на основе полученной от участников финансовой информации.

31. Схема осуществления авторизаций и клирингового обмена между участником и ОЦ и, участником и МПС указаны в Приложениях 1, 2 и зависят от технологической схемы взаимодействия.

32. Участники-эквайеры направляют клиринговые файлы в МПС.

33. МПС осуществляет обработку и клиринг полученных от участников файлов.

34. МПС направляет файлы с клиринговой информацией и соответствующие отчеты участникам напрямую.

35. МПС направляет NNSS Settlement файлы для расчетов с участниками в ОЦ.

36. ОЦ осуществляет расчет с участниками в рамках договоров о предоставлении услуг в межбанковской системе переводов денег по представленным МПС результатам национального межбанковского клиринга (KAZNNSS).

37. Гарантии расчетов по операциям несет МПС в соответствии с ее правилами.

9. Порядок обеспечения бесперебойности функционирования

38. Бесперебойное функционирование обеспечивается путем выполнения ОЦ и участниками следующего комплекса мер:

1) резервирование программно-технического комплекса, каналов связи и процессинговых центров участников (основной и резервный центры);

2) обеспечение резервного копирования и архивирования данных;

3) резервирование каналов связи – организация каналов связи от основного и резервного центров участника к ЦОД ОЦ;

4) постоянный мониторинг и анализ функционирования процессинговых центров участников с целью выявления причин и недопущения нарушений функционирования технологических средств, устройств, информационных систем;

5) проведение плановых профилактических работ, на оборудовании ОЦ и/или участников с обязательным информированием о проводимых работах сторонами;

6) обязательное тестирование в соответствии с планами восстановления функционирования процессинговых центров;

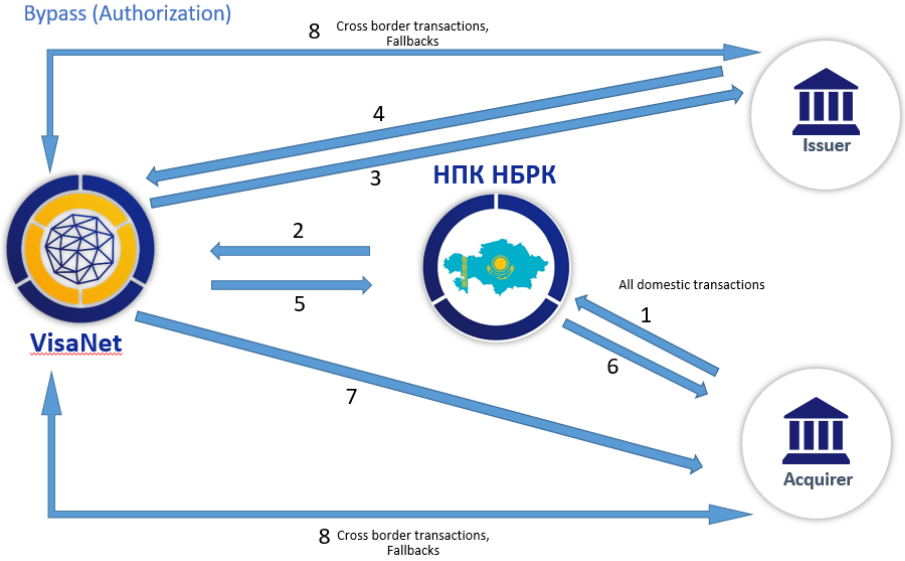
7) иные меры, направленные на обеспечение бесперебойности функционирования программно-технического комплекса, каналов связи и процессинговых центров участников.

39. Участники обеспечивают поддержку в активном состоянии каналов связи от своих процессинговых центров до ЦОД ОЦ.

40. В случае недоступности соединения участника-эквайера с ОЦ, участники самостоятельно переключаются на работу через канал МПС, принимая все необходимые меры по восстановлению соединения.

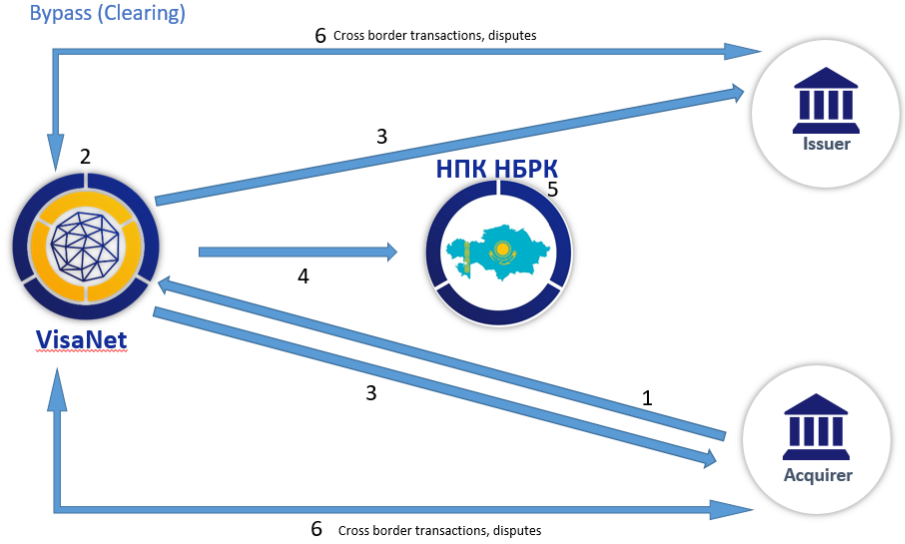
Приложение 1 к Руководству

Bypass (Authorization)



#	Описание процесса
1	Эквайер посылает авторизационный запрос в НПК в формате ISO 8583 Visa
2	НПК переправляет авторизационный запрос в VisaNet без изменений
3	VisaNet направляет авторизационный запрос Эмитенту
4	Эмитент направляет авторизационный ответ в VisaNet
5	VisaNet направляет авторизационный ответ в НПК
6	НПК возвращает авторизационный ответ Эквайеру
7	VisaNet направляет SMS репорты напрямую Эквайеру
8	Трансграничные операции, взаиморасчеты, диспутные операции продолжают функционировать в прежнем режиме.

Bypass (Clearing)



#	Описание процесса
1	Эквайер посылает файл-презентменты в VisaNet формате ISO 8583 Visa
2	VisaNet осуществляет клиринг
3	VisaNet направляет клиринговые файлы и VSS репорт банкам напрямую
4	VisaNet направляет NNSS Settlement файлы в НПК
5	НПК осуществляет расчет с банками
6	Трансграничные операции, взаиморасчеты, диспутные операции продолжают функционировать в прежнем режиме.

Приложение 2
к Руководству

Условия маршрутизации внутринациональных операций

Маршрутизация авторизационного запроса по карте МПС Visa осуществляется участником-эквайером в ОЦ при выполнении следующих условий:

- торгово-сервисное предприятие надлежащим образом зарегистрировано и осуществляет свою деятельность на территории Республики Казахстан;
- валюта транзакции – тенге.

Для технологий Visa Secure всех действующих протоколов аутентификационный поток для внутринацональных операций остается без изменений, а именно использование Visa Directory Server.