УТВЕРЖДЕН
решением Правления ПАО БАНК «СИАБ»
Протокол от «29» апреля 2022 г. № 36

ПРОТОКОЛ
(порядок информационного и технологического взаимодействия с использованием Универсального платежного шлюза)

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор безопасности Банка – сотрудник отдела информационной безопасности Банка, ответственный, в том числе, за формирование и обеспечение жизненного цикла ключей ЭП.

Администратор безопасности Провайдера – сотрудник отдела информационной безопасности Провайдера, ответственный, в частности, за организацию и проведение работ по обеспечению функционирования криптографических модулей (ПБЗИ) в Универсальном платежном шлюзе, в том числе, формирования и обеспечения жизненного цикла ключей ЭП.

Банк – Публичное акционерное общество «Санкт-Петербургский Индустриальный Акционерный Банк».

Владелец открытого ключа ЭП (Владелец ключа) – уполномоченное лицо любой из Сторон, создавшее криптографические ключи (закрытый и открытый), позволяющие создавать ЭП в электронных документах/электронных сообщениях (подписывать электронные документы/электронные сообщения ЭП). Созданный Владельцем открытый ключ ЭП должен быть передан Банком Провайдеру.

Выплата – банковская операция по переводу денежных средств в валюте Российской Федерации на Карту Получателя по Распоряжению Организации, осуществляемая с использованием Универсального платежного шлюза.

Информационный кабинет - программный модуль, предоставляемый Провайдером Банку, обеспечивающий информационный обмен между Банком и Провайдером и/или между Банком и Участником электронного взаимодействия. Информационный кабинет позволяет Банку и Участникам электронного взаимодействия контролировать Выплаты, Платежи и прочие параметры.

Карта - электронное средство платежа, используемое для совершения операций с денежными средствами, находящимися у Эмитента Карты.

Ключ проверки электронной подписи (открытый ключ) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи).

Ключ электронной подписи (закрытый ключ) – уникальная последовательность символов, предназначенная для создания электронной подписи.

Операция – *Платеж* или *Выплата*, осуществляемые через Универсальный платежный шлюз.

Отчетный день – календарный день, в течение которого осуществлялись Операции, установленный с 00 часов 00 минут 00 секунд до 23 часов 59 минут 59 секунд московского времени.

Отчетный период – календарный месяц с первого по последнее число месяца, в течение которого осуществлялись Операции.

ПБЗИ – Программная библиотека защиты информации.

Платеж – действия Банка в рамках применяемых форм безналичных расчетов по перечислению Организации денежных средств Плательщика, осуществляемые с использованием Универсального платежного шлюза.

Плательщик – физическое лицо, инициирующее осуществление Платежа.

Получатель – физическое лицо, имеющее договорные или иные отношения с Организацией, на основании которых Организация инициирует Выплату, являющееся держателем Карты, по реквизитам которой осуществляется Выплата.

Провайдер (Оператор услуг информационного обмена) – Общество с ограниченной ответственностью «Линксайд» (ОГРН 1187746670836), которому принадлежит Универсальный платежный шлюз.

Распоряжение – Электронный документ, направляемый Организацией Банку в целях осуществления Выплаты.

Система Провайдера (Система) – информационная система, состоящая из программно-аппаратного комплекса, включая Информационный кабинет, обеспечивающая информационное и технологическое взаимодействие между Банком и Участниками электронного взаимодействия.

Стороны – Банк, Провайдер, Участник.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Универсальный платежный шлюз – программно-аппаратный комплекс Провайдера, обеспечивающий осуществление Операций.

Участник электронного взаимодействия (Участник) – юридическое лицо (Организация), с которым Банком заключен договор, предметом которого является осуществление Банком Операций.

Электронный документ – информационный объект, состоящий из двух частей:

- реквизитной, содержащей процессинговые данные для осуществления платежей и выплат, а также ЭП;
- содержательной, включающей в себя текстовую, числовую информацию, которая обрабатывается в качестве единого целого.

В электронном документе содержится юридически значимая информация, направляемая Сторонами в электронной форме с использованием Универсального платежного шлюза.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Для целей настоящего Протокола под электронной подписью понимается

усиленная неквалифицированная электронная подпись, согласно Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Электронное сообщение – структурированная управляющая информация. В отличие от документа, сообщение генерируется автоматически и не имеет автора. Электронное сообщение подписывается ЭП. Электронное сообщение состоит из трех частей:

- строка сообщения – указывает метод передачи, URL-адрес, к которому нужно обратиться, и версию протокола HTTP;
- заголовки – описывают тело сообщения, передают различные параметры и др. сведения и информацию. В частности, в электронном сообщении присутствует заголовок «Authorization», к которому относится JWT;
- тело сообщения - данные, для передачи которых формируется сообщение.

Эмитент Карты – кредитная организация, заключившая с Получателем договор о выпуске Карты и осуществляющая расчеты по операциям, совершаемым с использованием Карты.

JWT – JSON Web Token. JSON-объект, который определен в открытом стандарте RFC 7519. JWT – Стандартизованный, подписанный и/или зашифрованный формат упаковки данных, используемый для безопасной передачи информации между Сторонами

Иные термины применяются в определениях, установленных договорами, заключенными между Банком и Участником, предметом которых является осуществление Банком Операций.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Протокол (порядок информационного и технологического взаимодействия с использованием Универсального платежного шлюза (далее – «Протокол») разработан на основании Гражданского кодекса Российской Федерации, Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», стандарта Р 50.1.031-2001 «Рекомендации по стандартизации. Информационные технологии поддержки жизненного цикла продукции. Терминологический словарь. Часть 1. Стадии жизненного цикла продукции».

2.2. Настоящий Протокол регламентирует общие принципы и порядок информационного и технологического взаимодействия и использования Участниками и Банком электронных документов и электронных сообщений посредством Универсального платежного шлюза в процессе исполнения договоров, заключенных между Участниками и Банком.

2.3. Порядок организации оборота электронных документов и электронных сообщений при осуществлении Участниками и Банком конкретных операций, формы используемых документов, правила их оформления определяются соответствующими договорами, заключенными между Участниками и Банком.

3. ПЕРИОД ДЕЙСТВИЯ ПРОТОКОЛА И ПОРЯДОК ВНЕСЕНИЯ В НЕГО ИЗМЕНЕНИЙ

3.1. Настоящий Протокол действует и является обязательным для Участников, заключивших договоры с Банком, в которых имеется условие о применении Протокола к отношениям Банка и Участника, на весь срок действия таких договоров.

3.2. Изменения (дополнения) в настоящий Протокол вносятся Банком в одностороннем порядке. Банк вправе определять сроки и порядок вступления в силу изменений (дополнений) в настоящий Протокол.

3.3. О внесении изменений (дополнений) в настоящий Протокол Банк уведомляет путем обязательного размещения указанных изменений (дополнений) на сайте Банка в сети Интернет по адресу: https://siab.ru

3.4. С целью обеспечения гарантированного ознакомления Участников с полным текстом изменений (дополнений) настоящего Протокола до вступления их в силу Участник обязан не реже одного раза в десять календарных дней обращаться на сайт Банка по адресу: https://siab.ru за сведениями об изменениях (дополнениях) в настоящий Протокол.

3.5. Участник имеет право получить в Банке текст Протокола и всех изменений (дополнений) к нему на бумажном носителе. Указанные в настоящем пункте документы должны быть предоставлены Участнику в течение пяти рабочих дней после получения соответствующего запроса.

4. ЭЛЕКТРОННЫЙ ДОКУМЕНТ И ЭЛЕКТРОННОЕ СООБЩЕНИЕ

4.1. В соответствии с настоящим Протоколом для подтверждения подлинности и авторства электронных документов/электронных сообщений Сторонами применяется электронная подпись (ЭП).

4.2. При исполнении любого договора между Участниками и Банком, в котором имеется условие о применении Протокола, обмен информацией и документами осуществляется путем пересылки электронных документов/электронных сообщений, подписанных ЭП отправителя. Электронные документы/электронные сообщения, получаемые Участниками через Универсальный платежный шлюз, заверяются ЭП Универсального платежного шлюза.

4.3. ЭП представляет собой реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием ключа ЭП (закрытого ключа ЭП) и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу ЭП (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа/электронного сообщения.

ЭП обладает следующими свойствами:

- воспроизводима только Владельцем ключа ЭП (уполномоченным сотрудником Участника, Банка, Провайдера);
- подлинность ЭП может быть удостоверена всеми Сторонами;
- ЭП неразрывно связана с конкретным электронным документом/электронным сообщением и только с ним.

4.4. Защита электронного документа средствами ЭП отправителя обеспечивает:

- проверку подлинности электронного документа/электронного сообщения;
- удостоверение личности отправителя.

4.5. Стороны признают и согласны с тем, что получение любых электронных документов/электронных сообщений, заверенных ЭП уполномоченных сотрудников Сторон с использованием Универсального платежного шлюза, юридически эквивалентно получению соответствующих документов на бумажных носителях, оформленных собственноручными подписями уполномоченных лиц сторон, заверенных печатями (в надлежащих случаях).

Стороны признают, что ЭП является аналогом собственноручной подписи (АСП) и соответствует всем критериям, предъявляемым к усиленной неквалифицированной подписи, требования к которой установлены Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и, соответственно, приравнивается Сторонами к усиленной неквалифицированной подписи.

Стороны признают и согласны с тем, что получение любых электронных документов/электронных сообщений, заверенных АСП, юридически эквивалентно получению соответствующих документов на бумажных носителях, оформленных собственноручными подписями уполномоченных лиц Сторон.

Примечание: Аналог собственноручной подписи (АСП) – реквизит Электронного документа (электронного сообщения), предназначенный для его защиты от подделки, полученный в результате криптографического преобразования информации с использованием закрытого (секретного) ключа и позволяющий идентифицировать владельца ключей как лицо, подписавшее документ (подтверждение авторства), а также установить отсутствие искажения информации в Электронном документе (подтверждение целостности электронного документа).

4.6. В соответствии с настоящим Протоколом для подтверждения подлинности электронных сообщений и аутентификации пользователей применяется JWT.

4.7. При исполнении любого договора между Сторонами, в котором содержится условие о применении Протокола, обмен данными осуществляется путем пересылки электронных сообщений, защищенных JWT.

4.8. Защита электронного сообщения JWT обеспечивает:

- проверку подлинности электронного сообщения;
- проверку подлинности (аутентификацию) отправителя (пользователя).
- удостоверение источника сообщения.

4.9. Универсальный платежный шлюз для создания пары «закрытый ключ - открытый ключ» использует ПБЗИ OpenSSL.

Для проверки ЭП используются соответствующие библиотеки языка программирования Golang.

Универсальный платежный шлюз, а также модули/библиотеки сайтов Организаций, использующие генерацию/проверку JWT, должны использовать алгоритмы, приведенные в "The JWT Handbook", Sebastián E. Peyrott.

4.10. Банк сохраняет Контрольный экземпляр программного обеспечения SignChecker.bin, разработанного Провайдером для проверки подлинности JWT, и предоставляет его копию по первому требованию Участника.

Стороны признают, что используемые ими средства электронной подписи, обеспечивающие формирование и проверку ЭП, контроль целостности, средства защиты электронных сообщений JWT и т.п. достаточным для обеспечения защиты электронного взаимодействия между Сторонами.

5. ПОРЯДОК СОЗДАНИЯ КЛЮЧЕЙ И ОБМЕНА ОТКРЫТЫМИ КЛЮЧАМИ

5.1. Администратор безопасности Провайдера обеспечивает для Участников возможность формирования (генерации) ключей ЭП путем предоставления ПО для генерации ключей, обеспечивает Участников необходимой документацией, обучением, поддержкой и обновлениями для ПО.

5.2. Открытый ключ и закрытый ключ ЭП со стороны Универсального платежного шлюза создается Администратором безопасности Провайдера и является частью договора с Участником.

5.3. Участник создает открытый и закрытый ключи ЭП в порядке, приведенном в Приложении № 1.

5.4 Ключи ЭП могут использоваться в следующих вариантах:

- Ключи ЭП, используются только для операций Платежи - срока действия не имеют.
- Ключи ЭП, используются только для операций Выплаты - срок действия не более 1 года.
- Ключи ЭП, используются как для операций Выплаты, так и для операций Платежи – срок действия не более 1 года.

5.5. Открытый ключ Участника, а также сведения о Владельце ключа ЭП доводятся до Банка на бумажном носителе за собственноручной подписью руководителя (уполномоченного лица) Участника, а так же дублируется в электронном варианте по электронной почте от ответственного представителя Участника ответственному представителю Банка.

5.6. Факт передачи открытого ключа подтверждается подписанием Акта, форма которого приведена в Приложении №2 к настоящему Протоколу. Подписание Акта сторонами означает взаимное признание ЭП с момента подписания Акта.

5.7. Открытый ключ со стороны Универсального платежного шлюза публикуется на официальном сайте Провайдера (https://4payments.com/docs/).

5.8 Данные электронных журналов (логов) Универсального платежного шлюза, формируемых программными средствами ПБЗИ и хранящихся на серверах Провайдера (протоколы операций), признаются Сторонами достаточными доказательствами совершения соответствующей операции (действия) в Универсальном платежном шлюзе.

6. ПОЛНОМОЧИЯ И ОТВЕТСТВЕННОСТЬ ВЛАДЕЛЬЦЕВ КЛЮЧЕЙ

6.1. Владелец ключа, назначенный Участником, обязан обеспечить выполнение общих требований:

- Обеспечить самостоятельно и за свой счет подключение своих электронно-вычислительных средств к сети Интернет, а также обеспечить защиту собственных электронно-вычислительных средств и ЭП от несанкционированного доступа и вредоносного программного обеспечения.
- Обеспечить, со своей стороны, наличие квалифицированного персонала для настройки и работы с Универсальным платежным шлюзом (включая ПБЗИ).
- Организовывать внутренний режим функционирования рабочих мест уполномоченных лиц таким образом, чтобы исключить возможность использования Универсального платежного шлюза и Ключей ЭП посторонними лицами.
- Извещать Банк и Провайдера, любым доступным способом, о компрометации ЭП, использовании Универсального платежного шлюза без его согласия и иных

нештатных ситуациях не позднее рабочего дня, следующего за днем обнаружения указанных событий.

Владелец ключа, назначенный Участником, обязан обеспечить выполнение требований информационной безопасности, указанных в разделе 7 данного документа.

6.2. При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Владелец ключа несет персональную ответственность за хранение личных ключевых носителей (ключей).

7. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Стороны обязуются предпринять все разумные меры для обеспечения Информационной безопасности Универсального платежного шлюза и сохранности своих закрытых ключей посредством применения программно-технических средств и организационных мер.

7.2. Стороны обязаны обеспечить:

- использование лицензионного программного обеспечения и его своевременное обновление;
- использование программного обеспечения, обеспечивающего защиту от вирусов, вредоносных программ, программ несанкционированного получения информации, и его своевременное обновление;
- использование средств межсетевого экранирования при подключении к сети общего пользования;
- сохранность и неизменность полученного программного обеспечения от Банка;
- доступ к Универсальному платежному шлюзу исключительно своих уполномоченных сотрудников;
- использование защищенных ключевых устройств (e-token, smart card или функциональные аналоги) для генерации и хранения закрытых ключей;
- при наличии технической возможности, использование технологии одноразовых паролей для подтверждения критичных операций;
- учет закрытых ключей;
- строгое сохранение владельцем ключа тайны закрытого ключа все время, включая момент создания ключа;
- внутреннее расследование каждого случая нарушения тайны закрытого ключа и принятие мер по результатам такого расследования.

7.3. Банк вправе приостановить работу Участника в Универсальном платежном шлюзе, если у него есть серьезные основания полагать, что информационная безопасность Участника нарушена (см. п. 7.7). В этом случае после устранения нарушений информационной безопасности Участника, Банк обязан восстановить работу Участника в Универсальном платежном шлюзе в минимально возможный срок.

7.4. Участник обязан эксплуатировать программное обеспечение Универсального платежного шлюза в соответствии с размещенной на официальном сайте Универсального платежного шлюза https://4payments.com/docs/ технической документацией и только для связи, с определенными в этой документации, серверами Универсального платежного шлюза.

7.5. Запрещается оставлять без контроля вычислительные средства с установленным ключевым носителем после ввода ключевой информации.

7.6. В случае невозможности отчуждения ключевого носителя с ключевой информацией от ПЭВМ организационно-техническими мероприятиями должен быть исключен доступ нарушителей к ПЭВМ с ключами.

7.7. Перечень критических событий, связанных с нарушением информационной безопасности в Системе Участника:

- компрометация ключей, т.е. потеря контроля доступа к ключам;
- потеря контроля над программным обеспечением;
- увольнение, перевод на другое место работы сотрудника, имевшего доступ к ключам;
- другие события, влияющие на безопасность обращения электронных документов и электронных сообщений.

7.8. При возникновении критического события Участник обязан незамедлительно осуществить блокирование скомпрометированных ключей.

7.8.1. В случае если Участник не обладает доступом к программному обеспечению по администрированию Владельцев ключей, он должен незамедлительно уведомить Банк об этом наиболее быстрым способом: по электронной почте, по факсимильной связи или иным образом по реквизитам, указанным на официальном сайте Банка.

7.8.2. В заявке на блокирование ключа должны быть указаны:

- полное наименование Участника;
- номер договора;
- реквизиты скомпрометированного ключа – его идентификатор в Универсальном платежном шлюзе;
- причина блокирования ключа.

7.8.3. ЭП электронных документов и электронных сообщений, отправленных в Универсальный платежный шлюз с момента блокирования указанного ключа, считается недействительной.

7.9. Исполнение заявок на блокирование ключей осуществляется Банком с 8 до 22 часов московского времени в течение одного часа после получения сообщения от Участника. Результатом исполнения заявки является прекращение проведения каких бы то ни было операций с использованием скомпрометированного ключа, направление Участником сообщения об этом по электронной почте.

7.10. В случае компрометации закрытого (секретного) ключа Банка Банк уведомляет Участника посредством размещения данной информации на информационном сервере Банка и рассылки соответствующего сообщения по электронной почте.

7.11. После получения уведомления о компрометации ключа ЭП Участник не должен использовать скомпрометированные ключи ЭП при выполнении проверки подлинности электронных документов и электронных сообщений, полученных после уведомления о компрометации, а также для подписания новых электронных документов и электронных сообщений.

8. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

8.1. В случае возникновения споров о подлинности электронных документов и электронных сообщений, подписанных ЭП, применяется процедура согласования разногласий, предусмотренная настоящим Разделом Протокола.

8.2. Бремя доказывания лежит на стороне, заявившей о нарушении ее прав и законных интересов.

8.3. Если одна из сторон утверждает, что электронный документ или электронное сообщение подписано ЭП, а другая эту ЭП не признает, то в 5 (пяти)-дневный срок путем обмена письмами стороны создают Согласительную комиссию. Полномочия членов Согласительной комиссии подтверждаются доверенностями. Председатель Согласительной комиссии не избирается, члены Согласительной комиссии равноправны.

8.4. Если стороны не договорятся об ином, в состав Согласительной комиссии входит равное количество представителей каждой из конфликтующих сторон, но не менее, чем по одному уполномоченному представителю.

8.5. В состав Согласительной комиссии, как правило, назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности сторон. Рекомендуется, чтобы эти лица обладали необходимыми знаниями в области построения системы электронного документооборота, работы компьютерных информационных систем. Также в состав Согласительной комиссии обязательно включается представитель/представители Провайдера.

8.6. По инициативе любой из сторон к работе Согласительной комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, соответствующие требованиям, указанным в п.8.5 настоящего Протокола, в том числе разработчики используемых в Универсальном платежном шлюзе средств защиты информации. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

8.7. После создания Согласительной комиссии стороны обязаны предоставить в Согласительную комиссию следующие материалы:

- сторона, принявшая и подтвердившая прием электронного документа либо электронного сообщения, предоставляет подписанный ЭП спорный электронный документ либо спорное электронное сообщение в виде файла;
- обе стороны предоставляют контрольные экземпляры открытого ключа ЭП в электронной форме, который используется ими при проверке подлинности оспариваемой ЭП, и документы, подтверждающие признание сторонами указанного открытого ключа ЭП;
- дополнительно могут быть представлены журналы (логи) взаимодействия участников с Универсальным платежным шлюзом - в части, касающейся спорной ситуации.

Банк предоставляет Контрольный экземпляр ПО для проверки подлинности ЭП.

8.8. Для проверки подлинности электронного документа или электронного сообщения Согласительная комиссия производит следующие действия:

- сравнивает открытые ключи ЭП, предоставленные сторонами. Верным признается экземпляр открытого ключа, комплементарный закрытому ключу ЭП стороны, подлинность ЭП которой оспаривается, и для которого имеются документы (например, Акт признания ключа подписи), подтверждающие признание сторонами указанного открытого ключа, действительные на момент формирования и отправки оспариваемого электронного документа или электронного сообщения;
- разворачивает проверочный стенд и устанавливает на нём Контрольный экземпляр программного обеспечения для проверки ЭП;

- проверяет правильность ЭП под спорным документом/сообщением, используя Контрольный экземпляр программного обеспечения, предназначенного для проверки ЭП.

8.9. Результаты работы Согласительной комиссии отражаются в акте, который подписывается всеми членами комиссии. Члены комиссии, несогласные с выводами большинства, подписывают указанный акт с возражениями, которые прилагаются к нему. Акт составляется в таком количестве экземпляров, чтобы каждая из конфликтующих сторон имела по одному подлинному экземпляру акта. По требованию члена комиссии ему может быть выдана заверенная копия акта.

8.10. ЭП признается фальшивой (недействительной) или подлинной (действительной) в зависимости от результатов проверки. Согласительная комиссия делает вывод о причинах возникновения разногласий и определяет виновную сторону.

8.11. Акт Согласительной комиссии является основанием для предъявления претензий к виновной стороне.

8.12. Акт Согласительной комиссии может быть представлен в качестве доказательства в случае разбирательства спора в судебных органах.

8.13. Порядок определения подлинности электронного документа, электронного сообщения и ЭП, установленный настоящим Протоколом, обязателен для Согласительной комиссии.

8.14. В случае уклонения какой-либо из сторон от создания Согласительной комиссии, другие стороны вправе самостоятельно назначить трех независимых экспертов для дачи заключения по вопросу подлинности спорной ЭП.

8.15. Письменное заключение экспертов составляется в таком количестве экземпляров, чтобы каждая из конфликтующих сторон имела по одному подлинному экземпляру.

8.16. Заключение экспертов может быть представлено в качестве доказательства в случае разбирательства спора в судебных органах.

8.17. Расходы по проведению согласительной процедуры оплачивает сторона, заявившая о нарушении ее прав и законных интересов.

8.18. В случае признания требований стороны, заявившей о нарушении ее прав и законных интересов, правомерными, виновная сторона обязана, в течение 5 (пяти) рабочих дней со дня, следующего за днем составления акта Согласительной комиссией или вынесения заключения экспертами, возместить другой стороне убытки в виде реального ущерба, наступившие в результате виновных действий, и расходы, связанные с проведением согласительной процедуры.

9. ИНЫЕ ПОЛОЖЕНИЯ

9.1. Стороны несут ответственность за действия своих сотрудников, уполномоченных Владельцев ключей ЭП, а также иных лиц, получивших или имеющих доступ (независимо от того, был ли этот доступ прямо санкционирован Участником или произошел помимо его воли) к аппаратным средствам, программному, информационному обеспечению, ключам ЭП и иным средствам, обеспечивающим оборот электронных документов и электронных сообщений в соответствии с настоящим Протоколом, как за свои собственные.

ПРИЛОЖЕНИЕ 1. ПОРЯДОК ФОРМИРОВАНИЯ КЛЮЧЕЙ АУТЕНТИФИКАЦИИ И JWT

Формирование открытого и закрытого ключей аутентификации

Для формирования пары ключей (закрытого и открытого) для работы с JWT используется ПБЗИ OpenSSL. Тип алгоритма, применяемый для формирования ЭП на основании данных, указанных в JWT Header и Claims: ES256 (согласно "The JWT Handbook", автор Sebastián E. Peyrott, версия 0.14.1).

Пример команды создания закрытого ключа:

```
openssl ecparam -name prime256v1 -genkey -noout -out private.pem
```

Пример команды для создания открытого ключа на основе закрытого ключа "private.pem":

```
openssl ec -in private.pem -pubout -out public.pem
```

Формирование JWT при платежах (тип операций Sale и Preauth)

Открытый ключ Участника является частью договора с Банком.

ЭП (неквалифицированная усиленная ЭП, согласно 63-ФЗ) является частью JW-токена в электронных сообщениях о платежах (согласно RFC 7519) и формируется на основании следующих данных:

1. Заголовок JW-токена:

```
{
  "alg": "ES256",
  "typ": "JWT"
}
```

2. Данные в Payload (JWT Claims):

- merchant_id - идентификатор ТСП
- shop_id - идентификатор магазина
- pub_key_id - идентификатор открытого ключа
- idempotency_key - ключ идемпотентности, уникальное значение для каждого запроса Участника
- amount.value - сумма платежа или пополнения
- amount.currency - валюта платежа или пополнения

Пример:

```
{
  "merchant_id": 1,
  "shop_id": 1,
  "pub_key_id":1,
  "idempotency_key ": 123abc,
  "amount": {
     "value": 10.01,
     "currency": "RUB"
   },
```

}

Формирование JWT при выплатах (тип операций Credit)

Открытый ключ Участника является частью договора с Банком.

ЭП (неквалифицированная усиленная ЭП, согласно 63-ФЗ) является частью JW-токена (согласно RFC 7519) и формируется на основании следующих данных:

1. Заголовок JW-токена:

```
{
  "alg": "ES256",
  "typ": "JWT"
}
```

2. Данные в Payload (JWT Claims):

- merchant_id - идентификатор ТСП
- shop_id - идентификатор магазина
- pub_key_id - идентификатор открытого ключа
- idempotency_key - ключ идемпотентности, уникальное значение для каждого запроса Участника
- amount.value - сумма выплаты
- amount.currency - валюта выплаты
- payout_method – структура, идентичная аналогичной из тела запроса, содержащая идентификатор/номер карты для выплаты

Пример:

```
{
  "merchant_id": 1,
  "shop_id": 1,
  "pub_key_id":1,
  "idempotency_key":123abc,
  "amount": {
     "value": 10.01,
     "currency": "RUB"
   },
"payout_method": {
      "card": {
       "number": "4000000000000002"
        }
   },
}
```

Формирование JWT при уведомлениях (тип операций Sale, Preauth и Credit)

Открытый ключ является частью договора с Банком, а также размещается на сайте Провайдера.

ЭП (НЭЦП согласно 63-ФЗ) является частью JW-токена в электронных уведомлениях (согласно RFC 7519) и формируется на основании следующих данных:

1. Заголовок JW-токена:

```
{
  "alg": "ES256",
  "typ": "JWT"
}
```

2. Данные в Payload (JWT Claims):

- payment_id или payout_id – идентификатор платежа или идентификатор выплаты
- merchant_id – идентификатор торгово-сервисного предприятия
- shop_id - идентификатор магазина
- amount.value - сумма операции
- amount.currency - валюта операции

Пример:

```
{
"payment_id": "449128d0-d867-4883-a8c7-e94571ef28e3",
"merchant_id": 1,
"shop_id": 1,
"amount": {
     "value": 10.01,
     "currency": "RUB"
   },
}
```

ПРИЛОЖЕНИЕ 2

ОБРАЗЕЦ

АКТ ПРИЕМА-ПЕРЕДАЧИ ОТКРЫТОГО КЛЮЧА ЭП

(_____)

г. Москва **«___» _____ 20____г.**

Акт приема-передачи открытого ключа ЭП подписывается руководителем Участника, действующего на основании Устава, и имеющим право на подписание доверенности от имени Участника .-В тексте Акта указывается полностью наименование должности, ФИО и паспортные данные уполномоченного сотрудника Участника. При оформлении Акта приема-передачи открытого ключа ЭП все стороны подписывают каждую страницу.

ПАО БАНК «СИАБ», именуемое в дальнейшем **«Банк»**, в лице _____, действующего на основании _____, с одной стороны, и

_____

_____,

именуемое в дальнейшем **«Участник»**, в лице _____

_____,

(ФИО руководителя)

действующего на основании Устава, с другой стороны, и уполномоченный сотрудник Участника_____

_____

_____,

(должность, ФИО Уполномоченного сотрудника полностью)

паспорт № _____ выдан _____

« » 20 г., именуемый в дальнейшем «Владелец ключей», с третьей стороны, составили настоящий Акт о нижеследующем:

1. Банк в соответствии с условиями Договора № от г. (далее по тексту - Договор) и Протоколом (порядок информационного и технологического взаимодействия с использованием Универсального платежного шлюза (далее – Протокол) зарегистрировал на имя Владельца ключа следующий Открытый ключ , сформированный с помощью ПБЗИ OpenSSL, и соответствующего ему Закрытого ключа:

ЗДЕСЬ ДОЛЖЕН БЫТЬ ОТКРЫТЫЙ КЛЮЧ

2. Указанный в п.1 настоящего Акта Открытый ключ используется для проверки ЭП в Электронных документах/электронных сообщениях, отправленных Участником в соответствии с Протоколом в период с момента подписания настоящего Акта проведения следующих операций:

☐ Ключ ЭП, используются только для операций **Платежи.** Срок действия Открытого ключа – не установлен.

☐Ключ ЭП, используются только для операций **Выплаты.** Срок действия Открытого ключа – не более одного года с момента подписания настоящего Акта.

☐Ключ ЭП, используются как для операций **Выплаты,** так и для операций **Платежи.** Срок действия Открытого ключа – не более одного года с момента подписания настоящего Акта.

3. Настоящим Актом Участник и Владелец ключей подтверждают, что Закрытый ключ, соответствующий указанному в п.1 настоящего Акта Открытому ключу:

- существует в единственном экземпляре и доступен только Владельцу ключа;

- используется Владельцем ключа для формирования ЭП в электронных документах/сообщениях от имени Организации в соответствии с вышеуказанным Протоколом.

4. Участник передал, а Банк получил указанный в п.1 настоящего Акта Открытый ключ в виде файла.
5. Подписание Акта Сторонами означает взаимное признание ЭП, вступающее в силу с момента подписания настоящего Акта.
6. Подписанием настоящего Акта Владелец ключа дает свое согласие на обработку (в том числе в автоматизированном режиме) Банком персональных данных Владельца ключа, содержащихся в настоящем Акте, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, а также иных действий, необходимых для обработки персональных данных Владельца ключа в рамках предоставления Банком услуг Участнику в соответствии с Протоколом. Срок действия согласия на обработку персональных данных: в течение срока действия Договора и затем в течение 5 (пяти) лет после окончания срока действия Договора.

Банк	**Участник**	**Владелец ключа**
_____ /_____/	_____ /_____/	_____ /_____/
м.п.	м.п.	