Правила использования Системы «Электронный Банк Digitale»

Оглавление

1. Термины

Термины, определенные в Соглашении об обслуживании в Системе «Электронный Банк» (далее – **Соглашение**) сохраняют свое значение при их использовании в настоящих Правилах. Дополнительно используются следующие термины:

1.1. **PUSH-сообщение** – короткое сообщение, направляемое Банком Клиенту, поступает на Мобильное устройство Клиента исключительно при наличии доступа к сети Интернет.

1.2. **QR-код** – оптическая метка, которая может содержать в т.ч. Ключ инициализации PayControl, компонент Ключа, инициализации PayControl, данные подтверждаемого ЭД.

1.3. **Авторизация** – подтверждение полномочий (предоставление прав доступа) Клиента, успешно прошедшего Аутентификацию входа.

1.4. **Акт признания ключа** – документ на бумажном носителе, подтверждающий принадлежность ключа проверки электронной подписи конкретному владельцу, оформляется по форме, установленной Приложением № № 1.

1.5. **Активация** – процедура персонализации Приложения PayControl, состоящая из следующих шагов:

1.5.1. ввод в Приложение PayControl Ключа инициализации PayControl;

1.5.2. формирование в Приложении PayControl и регистрации на сервере Банка набора уникальных признаков Мобильного устройства Клиента;

1.5.3. создание ключей (Ключ PayControl, Ключ проверки PayControl) в Приложении PayControl;

1.5.4. регистрация Ключа проверки PayControl на сервере Банка;

1.5.5. создание Клиентом Пароля/TouchID/FaceID для дальнейшего использования в качестве Аутентификационных данных.

1.6. **АРМ РКС** – автоматизированное рабочее место разбора конфликтных ситуаций. Используется для проверки подлинности ЭП при урегулировании разногласий. В зависимости от типа подписи используется АРМ РКС «КриптоПро» (для проверки УЭП), либо АРМ РКС «СэйфТек» (для проверки ПЭП PayControl).

1.7. **Аутентификационные данные –** Пароль/TouchID/FaceID, используемый для установления личности Пользователя при доступе к функциональности Приложения PayControl.

1.8. **Аутентификация входа** – процедура проверки соответствия предъявленных Аутентификационных данных Аутентификационным данным, установленным при активации Мобильного приложения. Выполняется перед началом работы в Приложении PayControl. Без успешной Аутентификации входа доступ к функциям подписи в Приложении PayControl не предоставляется.

1.9. **Группа А** – категория, определяющая право подписи Пользователя в Системе. Если полномочия «Группы А» предоставлены одному или нескольким Пользователям Клиента, и при этом ни одному из Пользователей этого Клиента не предоставлены

полномочия «Группы Б», ЭПД подписываются одной подписью любым Пользователем, отнесенным к «Группе А»[1].

1.10. **Группа Б** - категория, определяющая право подписи Пользователя в Системе. Если полномочия «Группы Б» предоставлены одному или нескольким Пользователям Клиента, то, как минимум, одному Пользователю этого Клиента должны быть предоставлены полномочия «Группы А». ЭПД подписываются двумя подписями. При этом одна подпись должна принадлежать «Группе А», а другая - «Группе Б»[1].

1.11. **Допустимый Временной Период** (**ДВП**) – временной период, в который могут быть совершены переводы денежных средств с использованием Системы. При использовании Клиентом ДВП, ЭПД Клиента принимаются в обработку только в течение ДВП. При направлении Клиентом в Банк ЭПД во время, не соответствующее ДВП, такие ЭПД Банком в обработку не принимаются. ДВП устанавливается по местному времени, действующему в городе месторасположения центрального офиса или регионального центра/филиала Банка, в котором обслуживается Клиент (Владивостокское, Новосибирское, Екатеринбургское или Московское время).

1.12. **Заявка** - заявка на установку параметров подключения к системе «Электронный Банк Digitale» (Приложение № 2 к Соглашению).

1.13. **Ключ проверки PayControl** – уникальная последовательность символов, служащая для проверки ПЭП PayControl. Вырабатывается на Мобильном устройстве Клиента одновременно с Ключом PayControl с использованием средства ЭП PayControl при выполнении процедуры Активации, а также при проведении плановой смены ключей PayControl. Однозначно соответствует Ключу PayControl. Хранится на Мобильном устройстве Клиента, а также передаётся на сервер PayControl, располагающийся в инфраструктуре Банка, для целей обеспечения процедуры Проверки ПЭП PayControl.

1.14. **Ключ PayControl** – уникальная последовательность символов, используемая для формирования ПЭП PayControl. Вырабатывается на Мобильном устройстве Клиента одновременно с Ключом проверки PayControl с использованием средства ЭП PayControl при выполнении процедуры Активации, а также при плановой смене ключей ЭП PayControl. Однозначно соответствует ключу проверки PayControl. Хранится на Мобильном устройстве Клиента и защищён средствами Мобильного приложения PayControl, средствами ОС Мобильного устройства и аппаратными средствами устройства.

1.15. **Ключи инициализации PayControl** – уникальные ключи, выпускаемые Банком для каждого Владельца ключей PayControl.

1.16. **Логин Пользователя** – уникальный универсальный идентификатор Пользователя в Подсистемах. Логин Пользователя назначается при подключении к Системе «Электронный Банк Digitale». Разрешается самостоятельная замена логина Пользователем средствами Системы.

1.17. **Приложение PayControl** – мобильное приложение для операционных систем iOS и Android, разработанное ООО «СэйфТек» (SafeTech LTD), выполняющее функции управления ключевой информацией (считывание, хранение, использование, обновление, удаление), получения информации для подтверждения от серверной

[1] В отношении ЭД, не являющихся платежными, например, ЭД типа соглашение/сделка, допускается использование только подписи Группы А, независимо от наличия или отсутствия Пользователей с правами Группы Б.

части, отображения подтвержденной информации на экране Мобильного устройства, выработки кода подтверждения на основе данных операции, ключа пользователя, времени обработки, отправки кода подтверждения в серверную часть.

1.18. **Мобильное устройство** – смартфоны, мобильные телефоны, планшеты и прочие устройства, на которых есть доступ в Интернет, установлены мобильное приложение Подсистемы «Мобильный клиент» и/или Приложение PayControl, и которые привязаны к Номеру телефона. Мобильное устройство используется, в том числе как носитель ключевой информации для средства ЭП PayControl.

1.19. **Номер телефона** – номер мобильного телефона Клиента для получения SMS-сообщений.

1.20. **Особая подпись** – категория, определяющая право подписи Пользователя в Системе и/или применяемый порядок использования Электронной Подписи в Системе[2]. Особая подпись назначается Пользователю в случае, когда его права по содержанию отличаются от категорий Группа А, Группа Б и Техническая подпись и/или порядок использования Пользователем в Системе Электронной Подписи имеет индивидуальные особенности. Содержание Особой подписи в каждом конкретном случае оговаривается Банком и Клиентом в Заявке на установку параметров подключения к системе «Электронный Банк Digitale» (Приложение № 2 к Соглашению).

1.21. **Перечень Допустимых Получателей** (**ПДП**) - перечень возможных получателей денежных средств (добровольное ограничение, которое может быть установлено по требованию Клиента). В адрес получателей, не входящих в ПДП, переводы не поддерживаются.

1.22. **Перечень Идентификаторов Допустимых Устройств** (**ПИДУ**) - перечень устройств, с использованием которых может осуществляться доступ Клиента/Пользователя к Системе с целью осуществления переводов денежных средств, на основе идентификаторов указанных устройств. При использовании ПИДУ, доступ к Системе с устройств, не входящих в ПИДУ, не предоставляется. В качестве идентификаторов устройств используется:

1.22.1. для Подсистемы «Интернет-Клиент»: IP-адрес и MAC-адрес;

1.22.2. для Подсистемы «Мобильный Клиент»: Pseudo-Unique ID (для мобильных устройств на базе Android) и Identifier for Vendor (IDFV, для iPhone).

1.23. **Проверка ПЭП PayControl** – процедура проверки соответствия предъявленной ПЭП данным ЭД, времени формирования ПЭП и набору уникальных признаков Мобильного устройства, выполняемая на сервере Банка.

1.24. **Средство ЭП PayControl** – программный комплекс, предназначенный для подписи/подтверждения уполномоченным лицом Клиента операций в Системе.

1.25. **Телефон Банка** – 8-800-700-1730, +7(495)775-83-42. Прием звонков обеспечивается в рабочие дни с 02:00 до 18:00 по Московскому времени. В дни, предшествующие праздничным и выходным дням, время приема звонков может быть сокращено.

1.26. **Техническая подпись** – категория, определяющая право подписи в Системе. При предоставлении полномочий «Техническая подпись» обеспечивается работа Пользователя с выписками и ЭД без права их подписи.

[2] Включая порядок дополнительного подтверждения ЭД (раздел 9 Правил).

1.27. **Формирование ПЭП PayControl** – процедура создания ЭП ЭД в Приложении PayControl на основе данных ЭД, времени формирования и набора уникальных признаков Мобильного устройства..

1.28. **Центр управления сертификатами** (**ЦУС**) – организационно–техническая система управления ключевой информацией Системы, включающая в себя:

1.28.1. персонал Банка, осуществляющий эксплуатацию и обеспечивающий работоспособность и информационную безопасность ЦУС;

1.28.2. программно-аппаратное обеспечение ЦУС;

1.28.3. программно-аппаратные средства защиты от несанкционированного доступа к ЦУС.

2. Пользователи и их полномочия в Системе

2.1. Список Пользователей Клиент сообщает Банку в Заявке.

2.2. Клиент подтверждает право Электронной подписи Пользователей и срок действия данного права одним из следующих способов:

2.2.1. в отношении лиц, которые в соответствии с нормами права действуют от имени Клиента без доверенности – выпиской из ЮГРЮЛ/ЕГРИП/торговой палаты, уставом, приказом о назначении на должность, иными документами. Если между Клиентом и Банком не оговорено иное, лица, действующие от имени Клиента без доверенности, получают право подписи Группы А;

2.2.2. в отношении прочих лиц - доверенностью по форме, установленной настоящими Правилами (Приложение № 2 к настоящим Правилам). В случае использования доверенности допускается применение формы, отличной от установленной Приложением № 2 к настоящим Правилам, при условии, что по содержанию доверенности можно однозначно установить полномочия Пользователя. Решение о допустимости использования формы доверенности, предложенной Клиентом, в каждом конкретном случае принимает Банк. При этом Банк имеет право взимать плату за обработку формы доверенности, предложенной Клиентом. Лица, действующие от имени Клиента по доверенности, получают право подписи, указанное в доверенности.

2.3. Для изменения содержания прав действующих Пользователей Клиент предоставляет в Банк документы, указанные в п.п. 2.2.1, 2.2.2.

2.4. В случае изменения списка Пользователей Клиент представляет в Банк новую Заявку.

2.5. Если в Заявке указаны новые Пользователи, то их права и срок действия прав подтверждаются документами, указанными в п.п. 2.2.1, 2.2.2.

2.6. При получении новых комплектов документов, подтверждающих права Пользователей, Банк обеспечивает приведение полномочий Пользователей Клиента в соответствии с новыми документами не позднее, чем на третий рабочий день с момента получения документов.

2.7. Если заблаговременная подача Заявки, документов, подтверждающих изменения полномочий, невозможна, в отношении Пользователей, полномочия которых прекращены/ограничены, Клиент дополнительно применяет порядок действий, установленный п. 10.2.

3. Усиленная Электронная Подпись

3.1. Владельцами Усиленной Электронной Подписи (УЭП) и Сертификатов ключей проверки электронной подписи (СКП) в Системе являются Пользователи, имеющие право Электронной подписи.

3.2. Создание ключей УЭП производится Владельцем СКП самостоятельно с использованием Системы. Банк не участвует в процедуре создания ключей УЭП Клиента и не имеет к ним доступа. Создание ключей УЭП может выполняться в связи с: началом работы в Системе, истечением срока действия используемого ключа, решением Владельца СКП в целях повышения информационной безопасности, а также в других случаях.

3.3. Создание ключей УЭП сопровождается направлением в Банк посредством Системы электронного запроса на выпуск СКП.

3.4. Ключ (и соответствующий ему СКП) конкретного Владельца СКП может быть Первым или Очередным.

3.5. Первым ключом (и соответствующим ему СКП) считается ключ (СКП), созданный Владельцем СКП без использования действующего ключа. При создании Первого ключа Клиент оформляет и представляет в Банк Акт признания ключа проверки ЭП.

3.6. Очередной ключ (и соответствующий ему СКП) создается при наличии у Владельца СКП действующего Первого или Очередного ключа. При этом направляемый в Банк запрос на выпуск СКП подписывается действующим Первым или Очередным ключом УЭП.

3.7. Банк выпускает Клиенту СКП на основании запроса на СКП, полученного по Системе.

3.8. Банк разрешает использование Клиентом Первого ключа только при условии предоставления Клиентом в Банк оригинала Акта признания ключей.

3.9. Первый СКП признается принадлежащим конкретному Владельцу СКП, если запрос, на основании которого выпущен Первый СКП, подписан ключом, указанным в Акте признания ключей.

3.10. Очередной СКП признается принадлежащим конкретному Владельцу СКП, если:

3.10.1. в соответствии с п. 3.9 установлена принадлежность Первого СКП данному Владельцу СКП;

3.10.2. последовательно может быть установлена подлинность ЭП электронных запросов, направленных в Банк в соответствии с п. 3.6, на все Очередные СКП данного Владельца СКП, вплоть до электронного запроса на СКП, принадлежность которого необходимо установить.

3.11. Срок действия ключа (Первого, Очередного) и соответствующего ему СКП указывается в СКП.

3.12. Применяемые в Системе программные средства работы с СКП в процессе их использования автоматически выполняют контроль срока действия СКП. СКП с истекшим сроком действия не может быть использован для осуществления документооборота в Системе.

3.13. Банк обеспечивает хранение СКП Клиентов в форме электронных документов и возможность получения СКП Клиентов в форме электронных документов или в форме документов на бумажных носителях в течение 10 (десяти) лет с момента их выпуска.

4. Простая Электронная Подпись PayControl

4.1. Общие положения:

4.1.1. Банк не контролирует, не проверяет, не дает одобрения и не несет какой-либо ответственности за иные приложения, кроме Приложения PayControl и приложения подсистемы «Мобильный Клиент», добавляемые Клиентом на свое Мобильное устройство.

4.1.2. Клиент и Банк признают ПЭП PayControl равнозначной собственноручной подписи Клиента.

4.1.3. Средство ЭП PayControl является средством простой ЭП.

4.1.4. Стороны признают применение Средства ЭП PayControl в Системе достаточным для обеспечения целостности, авторства и неотказуемости передаваемой между Сторонами информации и невозможности ее фальсификации после момента её подписания.

4.2. Выпуск ключей – общие правила.

4.2.1. Перед выпуском ключей Клиент должен выполнить требования технической защиты к Мобильному устройству и установку Приложения PayControl из одного из официальных репозиториев Google Play или App Store.

4.2.2. Ключи инициализации ЭП PayControl выпускаются Банком для каждого Владельца ключа PayControl.

4.2.3. Допускаются следующие способы передачи Ключей инициализации Pay Control Банком Владельцу ключа:

4.2.3.1. Передача одним сообщением в виде QR-кода, который передается путем вывода на экран монитора;

4.2.3.2. Передача двумя сообщениями/частями:

4.2.3.2.1. первая часть - в виде QR-кода путем вывода на экран монитора;

4.2.3.2.2. вторая часть - в виде SMS или сообщения на e-mail.

4.2.4. После внесения в Приложение PayControl Ключей инициализации PayControl, система PayControl выполняет автоматическую процедуру выпуска Ключа PayContropl с сохранением его в зашифрованном виде в Мобильном устройстве, отправку в Банк значения Ключа проверки PayControl и инициализацию Ключа проверки PayControl в Банке.

4.2.5. Ключ PayControl может быть первым (п.4.3) или очередным (п.4.4).

4.3. Первый ключ PayControl.

4.3.1. Первый ключ PayControl – это ключ, созданный без использования действующего Ключа PayControl.

4.3.2. Для Первого ключа PayControl оформляется Акт признания ключа проверки ЭП PayControl.

4.3.3. Банк формирует Акт признания ключа проверки ЭП автоматически после успешного завершения действий, указанных в п.4.2.4.

4.3.4. Клиент должен проверить полученный Акт, в т.ч. убедиться в совпадении значений идентификатора пользователя и Ключа проверки PayControl, отображаемыми в Приложении PayControl, со значениями в Акте.

4.3.5. В зависимости от того, имеет ли владелец выпускаемого Первого ключа действующий ключ/СКП УЭП, Акт может быть оформлен одним из способов:

4.3.5.1. Если действующий ключ/СКП УЭП отсутствует, Клиент оформляет и передает документы в Банк на бумажных носителях.

4.3.5.2. Если действующий ключ/СКП УЭП имеется:

4.3.5.2.1. Владелец может подписать сформированный Акт в электронной форме действующим ключом УЭП и направить подписанный Акт в Банк посредством Системы.

4.3.5.2.2. Клиент может оформить Акт на бумажном носителе, как указано в п.4.3.5.1.

4.3.6. После успешной проверки Акта Банком, Банк разрешает использование Первого ключа PayControl.

4.3.7. Для Первого ключа PayControl подпись признается совершенной конкретным Владельцем ключа, если:

4.3.7.1. на данного владельца оформлен Акт признания ключа проверки ЭП PayControl;

4.3.7.2. Ключ проверки PayControl, указанный в Акте, позволяет успешно проверить данную подпись.

4.4. Очередной ключ PayControl.

4.4.1. Очередной ключ PayControl – это ключ, созданный на основании запроса на продление ключа PayControl.

4.4.2. Очередной ключ PayControl выпускается [включая, но не ограничиваясь] в связи с приближением даты прекращения действия имеющегося Ключа PayControl.

4.4.3. Запрос на продление ключа PayControl Владелец ключа создает самостоятельно, подписывает действующим (Первым или Очередным) ключом PayControl и направляет в Банк по Системе.

4.4.4. На основании полученного запроса Банк запускает процедуру выпуска Очередного ключа PayControl, которая выполняется в соответствии с п.п. 4.2.2, 4.2.3, 4.2.4.

4.4.5. Для Очередных ключей PayControl Акт признания ключа проверки ЭП PayControl не оформляется.

4.4.6. Для Очередного ключа PayControl подпись признается совершенной конкретным Владельцем, если:

4.4.6.1. проверена согласно 4.3.7 подпись первого запроса на продление ключа PayControl;

4.4.6.2. последовательно проверена подлинность всех запросов на продление ключа PayControl, направленных в Банк в соответствии с п. 4.4.3, вплоть до того ключа, которым совершена подпись проверяемого ЭД.

4.5. Порядок совершения ПЭП PayControl.

4.5.1. Банк на основании запроса Клиента формирует и направляет Клиенту Электронное сообщение с шаблоном ЭД.

4.5.2. Одновременно на Мобильное устройство Клиента направляется PUSH-сообщение о необходимости подписания ЭД.

4.5.3. Клиент проходит Аутентификацию входа в Приложении PayControl.

4.5.4. В Приложении PayControl Клиенту отображается Электронное сообщение Банка с шаблоном ЭД.

4.5.5. Клиенту предоставляется возможность подписать ЭД средством ЭП PayControl или отказаться от подписи.

4.5.6. Если Клиент нажимает кнопку «Отказаться», ЭД не будет подписан ЭП и не будет направлен на исполнение в Банк.

4.5.7. Если Клиент нажимает кнопку «Подтвердить», то с помощью Приложения PayControl ЭД подписывается и направляется на исполнение в Банк.

4.5.8. Банк выполняет проверку ПЭП PayControl и, в случае успеха, принимает ЭД в обработку.

4.5.9. Если Клиент не принял решение о совершении подписи (не нажал ни одну из кнопок) в течение установленного времени с момента получения соответствующего Электронного сообщения от Банка, такое Электронное сообщение аннулируется и исчезает из списка операций в Приложении PayControl.

4.6. Особенности совершения ПЭП PayControl в режиме off-line.

4.6.1. Под режимом off-line понимается ситуация, в которой на Мобильном устройстве [временно] отсутствует доступ в Интернет.

4.6.2. В режиме off-line допускается совершение ПЭП PayControl в следующем порядке.

4.6.3. Подсистема «Интернет клиент»/«Мобильный клиент» отображает данные подписываемого ЭД в форме QR-кода.

4.6.4. Клиент проходит Аутентификацию входа в Приложении PayControl.

4.6.5. Клиент вносит данные подписываемого ЭД в Приложение PayControl путем считывания QR-кода (п.4.6.3).

4.6.6. Приложение PayControl отображает данные подписываемого ЭД и вычисляет код подтверждения - уникальный код проверки целостности информации, позволяющий гарантировать неизменность данных после подписания.

4.6.7. Клиент вносит код подтверждения в подсистему «Интернет клиент»/ «Мобильный клиент».

4.6.8. Банк выполняет проверку ПЭП PayControl и, в случае успеха, принимает ЭД в обработку.

4.7. В целях управления рисками Банк может ограничивать суммы Электронных Платежных Документов, доступных для подписи ПЭП PayControl. Значения используемых ограничений доводятся до Клиента путем Публичного размещения информации.

5. Простая Электронная Подпись OTP

5.1. OTP (One-Time Password, одноразовый пароль) – это последовательность символов, которая направляется Клиенту (Пользователю) в автоматическом режиме в форме SMS-сообщения.

5.2. С 01.03.2021 г. возможность использования ПЭП ОТР новым пользователям не предоставляется. Вместо этого должны использоваться ПЭП PayControl и/или УЭП.

5.3. Каждый одноразовый пароль имеет ограниченный срок действия, который устанавливается Банком.

5.4. ПЭП ОТР проставляется путем ввода Клиентом в Систему ОТР для конкретного ЭД.

5.5. В целях управления рисками Банк ограничивает суммы Электронных Платежных Документов, доступных для подписи ПЭП ОТР. Значения используемых ограничений доводятся до Клиента путем Публичного размещения информации.

6. Подсистема «Интернет-Клиент»

6.1. Подсистема «Интернет-Клиент» обеспечивает безналичное расчетное и информационное обслуживание Клиента через защищенный Интернет-сайт Банка путем обработки и исполнения Электронных документов, передаваемых со стороны Клиента и подписанных Усиленной Электронной Подписью (УЭП) и (или) Простой Электронной Подписью (ПЭП) Клиента.

6.2. При использовании УЭП принимаются в обработку следующие типы Электронных документов.

6.2.1. электронный запрос на выпуск СКП;

6.2.2. платежное поручение, в т.ч. в форме массового платежа, когда несколько платежных поручений подписаны одной УЭП;

6.2.3. заявление на перевод в иностранной валюте[3];

6.2.4. заявление на покупку иностранной валюты;

6.2.5. заявление на продажу валюты за рубли/другую иностранную валюту;

6.2.6. запрос на выписку;

6.2.7. распоряжение на списание средств с транзитного валютного счета[3];

6.2.8. справка о подтверждающих документах[3];

6.2.9. сведения о валютных операциях;

6.2.10. контракт для постановки на учет;

6.2.11. кредитный договор для постановки на учет;

6.2.12. заявление об изменении сведений о контракте (кредитном договоре);

6.2.13. заявление о снятии с учета контракта (кредитного договора);

6.2.14. ЭД типа соглашение/сделка[3]

6.2.15. заявление о предоставлении кредитного транша[4];

6.2.16. заявление о полном/частичном акцепте, отказе от акцепта распоряжения получателя средств[4];

6.2.17. заявление на открытие аккредитива[4];

6.2.18. поручение на выдачу банковской гарантии[4];

[3] в том числе, с прикрепленными документами

[4] при наличии технической возможности

6.2.19. инкассовое поручение[4];

6.2.20. письма в свободном формате[3], за исключением документов, связанных с продлением полномочий Пользователей, внесением изменений в карточку с образцами подписей и оттиска печати и уставные документы, а также изменением иных данных Клиента, имеющихся в Банке.

6.2.21. запрос на отзыв ЭД;

6.2.22. Акт признания ключа проверки ЭП PayControl[4/]

6.3. При использовании ПЭП принимаются в обработку следующие типы Электронных документов:

6.3.1. при использовании PayControl:

6.3.1.1. заявление на перевод в рублях;
6.3.1.2. заявление на перевод в рублях в форме массового платежа;
6.3.1.3. запрос на продление ключа PayControl;
6.3.1.4. документы, перечисленные в п.п. 6.2.3- 6.2.21.

6.3.2. при использовании OTP:

6.3.2.1. заявление на перевод в рублях;
6.3.2.2. запрос на отзыв ЭД.

6.4. При получении от Клиента через Систему заявления на перевод в рублях, в Банке на основании данного заявления формируется и исполняется платежное поручение. Клиент поручает уполномоченным сотрудникам Банка подписывать от имени Клиента платежные поручения, составленные на основании указанных заявлений.

6.5. Многоразовые пароли:

6.5.1. Пароль интернет-пользователя используется для входа в Подсистему «Интернет-Клиент».

6.5.1.1. Пользователь может в любой момент самостоятельно изменить пароль интернет-пользователя вне зависимости от источника его происхождения.
6.5.1.2. Первый пароль интернет-пользователя передается Клиенту в форме SMS-сообщения на номер, указанный Клиентом согласно п. 8.1.1.
6.5.1.3. В случае утраты пароля интернет-пользователя (забыл пароль), Банк по запросу Пользователя передает ему новый пароль в порядке, указанном в п. 6.5.1.2.
6.5.1.4. После первого использования пароля интернет-пользователя, переданного Пользователю Банком (согласно п.п. 6.5.1.2 и 6.5.1.3), Пользователь обязан самостоятельно его заменить.

6.5.2. Для работы с ключом подписи используется пароль к носителю ключа/к контейнеру с ключом ЭП.

6.5.2.1. В случае получения носителя ключа в Банке Клиент получает вместе с ним пароль к носителю ключа.
6.5.2.2. Клиент (Пользователь) должен самостоятельно после первого использования заменить пароль к носителю ключа, полученный в Банке.
6.5.2.3. Во всех случаях, кроме указанных в п.п. 6.5.2.1 и 6.5.2.2, Клиент (Пользователь) создает пароль к носителю ключа/к контейнеру с ключом ЭП самостоятельно.

6.5.2.4. Пользователь может в любой момент самостоятельно изменить пароль к носителю ключа/к контейнеру с ключом ЭП вне зависимости от источника его происхождения.

6.6. Клиент Системы «Электронный Банк» допускается к безналичному расчетному и информационному обслуживанию через Подсистему «Интернет-Клиент» после выполнения им всей совокупности следующих действий:

6.6.1. ознакомление с условиями Соглашения и настоящих Правил;

6.6.2. оформление Заявки;

6.6.3. подтверждение права Электронной подписи Пользователей в соответствии с п. 2.2;

6.6.4. подготовка рабочего места в соответствии с требованиями Приложения № № 3 к настоящим Правилам;

6.6.5. установка Подсистемы «Интернет-Клиент» на стороне Клиента и получение сообщения из Банка о готовности банковской части Системы к началу работы в Подсистеме «Интернет-Клиент»;

6.6.6. выполнение полуавтоматической процедуры по созданию логина и пароля Интернет-пользователя.

6.7. Уведомления об Операциях ЭСП (Уведомления):

6.7.1. Уведомления Клиенту направляются путем отображения соответствующего Статуса ЭД в электронных формах «все документы → Исходящие документы» Подсистемы «Интернет-Клиент».

6.7.2. Уведомлением является запись в электронной базе данных, содержащая информацию об Операции ЭСП.

6.7.3. Уведомление доступно Клиенту для получения с момента принятия Банком ЭПД в обработку.

6.8. Ограничение максимальной суммы переводов денежных средств по требованию Клиента:

6.8.1. Клиент имеет право ограничить максимальную сумму переводов денежных средств, осуществляемых с использованием Системы, по каждому отдельно взятому Счету системы.

6.8.2. В целях установки такого ограничения Клиент обращается в Банк с надлежащим образом оформленной Заявкой.

6.8.3. Банк вводит в действие запрашиваемые Клиентом ограничения не позднее, чем через 5 (пять) рабочих дней с момента приема Заявки от Клиента.

6.8.4. Если сумма перевода денежных средств, осуществляемого посредством Системы, превышает установленные ограничения, Банк отказывает в исполнении такого перевода.

6.9. Перечень Допустимых Получателей (ПДП):

6.9.1. Клиент имеет право установить ПДП.

6.9.2. Для установки ПДП и отказа от использования ПДП Клиент обращается в Банк с соответствующим образом оформленной Заявкой.

6.9.3. Банк настраивает для Клиента возможность использования ПДП в соответствии с Заявкой в срок, не превышающий 5 (пять) рабочих дней с момента представления такой Заявки в Банк, и уведомляет Клиента о завершении настройки сообщением через Систему.

6.9.4. По завершении настройки согласно п. 6.9.3 Клиент формирует ПДП самостоятельно с использованием Системы.

6.9.5. ПДП формируется посредством подписания ЭП Клиента записей справочников корреспондентов и бенефициаров (ПДП подписывается ЭП Клиента).

6.9.6. Система обеспечивает соблюдение на стороне Клиента принципа «четырех глаз» при формировании ПДП: создание записей справочников корреспондентов и бенефициаров и их подписание ЭП не может быть выполнено одним и тем же Пользователем.

6.9.7. Система обеспечивает невозможность подписания ЭП Клиента, а также невозможность принятия в Банке платежного поручения/заявления на перевод в иностранной валюте, если используется получатель/бенефициар, отличный от подписанных ЭП Клиента записей в справочнике корреспондентов/бенефициаров.

6.10. Перечень Идентификаторов Допустимых Устройств (ПИДУ) и Допустимый Временной Период (ДВП):

6.10.1. Клиент имеет право установить ПИДУ/ДВП.

6.10.2. Для установки, внесения изменений в ПИДУ/ДВП и отказа от использования ПИДУ/ДВП Клиент обращается в Банк с соответствующим образом оформленной Заявкой.

6.10.3. Банк настраивает для Клиента ПИДУ/ДВП в соответствии с Заявкой в срок, не превышающий 5 (пять) рабочих дней с момента представления такой Заявки в Банк.

6.10.4. После завершения настройки согласно п. 6.10.3 доступ Клиента к Подсистеме обеспечивается только с устройств, удовлетворяющих ПИДУ, а прием от Клиента ЭПД осуществляется только в ДВП.

7. Подсистема «Мобильный Клиент»

7.1. Подсистема «Мобильный Клиент» обеспечивает безналичное расчетное и информационное обслуживание Клиента путем использования Клиентом функций мобильного приложения, устанавливаемого на Мобильном устройстве при применении Простой Электронной Подписи.

7.2. Для получения обслуживания в полном объеме, в частности, для использования функций, перечисленных в п.п. 7.8, 7.9 и 7.10, Клиент должен одновременно с Подсистемой «Мобильный Клиент» использовать Подсистему «Интернет-Клиент».

7.3. Подсистема «Мобильный Клиент» обеспечивает обработку следующих видов Электронных документов, передаваемых со стороны Клиента и подписанных Электронной подписью Клиента:

7.3.1. заявление на перевод в рублях;

7.3.2. запрос на отзыв платежного поручения;

7.3.3. письма в свободном формате (только для ПЭП PayControl).

7.4. В отношении заявления на перевод в рублях действуют условия, указанные в п. 6.4.

7.5. Многоразовые пароли, коды и биометрические средства аутентификации.

7.5.1. Для первого входа в Подсистему «Мобильный Клиент» используется пароль интернет-пользователя (п. 6.5.1).

7.5.2. Код доступа к Подсистеме «Мобильный Клиент» - это четырехзначное число, которое Пользователь назначает самостоятельно с использованием Подсистемы. При назначении первого кода доступа Пользователь предъявляет пароль интернет-пользователя (п. 6.5.1). При назначении последующих кодов доступа Пользователь предъявляет действующий код доступа.

7.5.3. При наличии кода доступа (п. 7.5.2) допускается использование для входа в Подсистему биометрических средств аутентификации, поддерживаемых Мобильным устройством Пользователя (по отпечатку пальца или по лицу Пользователя).

7.5.4. В случае нежелания/невозможности использования кода доступа (п. 7.5.2)/биометрических средств аутентификации (п. 7.5.3) Пользователь использует для входа в Подсистему пароль интернет-пользователя (п. 6.5.1).

7.6. Клиент допускается к работе с Подсистемой «Мобильный Клиент» после выполнения им всей совокупности следующих действий:

7.6.1. ознакомление с условиями Соглашения и настоящих Правил;

7.6.2. оформление Заявки;

7.6.3. подтверждение права Электронной Подписи Пользователей в соответствии с п. 2.2;

7.6.4. подготовка рабочего места в соответствии с требованиями Приложения № № 3 к настоящим Правилам;

7.6.5. получение сообщения из Банка о готовности банковской части Системы к обслуживанию Клиента в Системе;

7.6.6. скачивание Клиентом из репозиториев Apple Store/Play Market мобильного приложения Digitale Банка Интеза и установка его на Мобильное устройство Клиента.

7.7. Ограничение максимальной суммы переводов денежных средств по требованию Клиента:

7.7.1. Клиент вправе установить в порядке, определенном в п. 6.8, дополнительные ограничения на максимальные суммы переводов денежных средств.

7.8. Уведомления об Операциях ЭСП, совершенных с использованием Подсистемы «Мобильный Клиент», направляются через Подсистему «Интернет-Клиент» по правилам, указанным в п. 6.7.

7.9. Использование Перечня Допустимых Получателей (ПДП) осуществляется по правилам, указанным в п. 6.9. При этом самостоятельное формирование Клиентом ПДП выполняется в Подсистеме «Интернет-Клиент».

7.10. Использование Перечня Идентификаторов Допустимых Устройств (ПИДУ) и Допустимого Временного Периода (ДВП) осуществляется согласно п. 6.10.

8. Сообщения: SMS и e-mail

8.1. Номера телефонов для получения SMS.

8.1.1. SMS-сообщения направляются на номера мобильных телефонов:

8.1.1.1. указанные Клиентом в надлежащим образом оформленной Заявке;
8.1.1.2. указанные Клиентом в запросе, направленном в Банк через Систему в форме письма в свободном формате, подписанного УЭП или ПЭП PayControl;

8.2. Адреса для получения e-mail.

8.2.1. Сообщения e-mail направляются на адреса:

8.2.1.1. указанные Клиентом в надлежащим образом оформленной Заявке.
8.2.1.2. указанные Клиентом в запросе, направленном в Банк через Систему в форме письма в свободном формате, подписанного УЭП или ПЭП PayControl.

8.3. Базовые сообщения.

8.3.1. Базовыми являются сообщения, необходимые для использования Клиентом Системы.

8.3.2. Базовые сообщения направляются Клиенту без взимания дополнительной платы.

8.3.3. Базовые сообщения используются для отправки Клиенту:

8.3.3.1. Логина Пользователя посредством e-mail (п. 1.16);
8.3.3.2. пароля Интернет-пользователя посредством SMS (п.п. 6.5.1, 7.5.1);
8.3.3.3. одноразовых паролей посредством SMS;
8.3.3.4. номера лицензии СКЗИ посредством SMS/e-mail;
8.3.3.5. инструкций по установке, настройке и использованию Системы посредством e-mail.

8.4. Расширенные сообщения.

8.4.1. Расширенными являются сообщения, которые не являются необходимыми для использования Клиентом Системы.

8.4.2. Расширенные сообщения используются для предоставления Клиенту оперативной информации о событиях, связанных с Системой.

8.4.3. Банк может устанавливать в Тарифах и взимать плату за предоставление расширенных сообщений.

8.5. Ограничение ответственности Банка в отношении SMS и e-mail.

8.5.1. В соответствии с настоящими Правилами Клиент предоставляет Банку право направлять информацию, указанную в п. 8 Правил, посредством отправки SMS, и e-mail.

8.5.2. Банк обеспечивает возможность настройки параметров расширенных сообщений (п. 8.4), в том числе выбор из списка событий, в отношении которых отправляются сообщения, и настройку параметров для отправки таких сообщений.

8.5.3. Клиент обязуется принимать достаточные и необходимые меры для защиты информации, отправляемой путем SMS и e-mail, и ограничения доступа к такой информации неуполномоченных лиц.

8.5.4. Клиент освобождает Банк от ответственности за ненадлежащее исполнение обязательств в части отправки SMS и e-mail в случае, если это обусловлено техническими сбоями в сетях операторов связи, действиями операторов связи, нарушениями в электроснабжении и работе программно-технических средств, используемых Банком.

9. Дополнительное подтверждение Электронного Документа

9.1. В процессе обработки в Системе отдельных Электронных документов, полученных от Клиента, в целях информационной безопасности Банк может запросить у Клиента дополнительное подтверждение Электронного документа в форме ПЭП или одноразового пароля.

9.2. Если для конкретного Электронного документа запрошено дополнительное подтверждение, Банк имеет право не проводить обработку этого документа до момента получения запрошенного подтверждения.

10. События компрометации

10.1. События компрометации включают:

10.1.1. компрометацию ключа ЭП – событие, в результате которого возможно несанкционированное Владельцем использование ключа ЭП. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь: потеря ключевых носителей; потеря ключевых носителей с их последующим обнаружением; увольнение сотрудников, имевших доступ к ключевой информации; нарушение правил хранения носителей ключевой информации; получение доступа к носителям ключевой информации лицами, не являющимися Владельцами соответствующих СКП; случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

10.1.2. утрату устройства, обеспечивающего прием SMS-сообщений;

10.1.3. случаи, когда устройство, обеспечивающее прием SMS-сообщений, стало доступным для использования третьим лицам;

10.1.4. получение паролей/расширенных сообщений о входе в Систему в ситуациях, когда сам Клиент не предпринимал попыток входа в Систему;

10.1.5. получение информации о расходных операциях, которые были совершены без согласия Клиента (информация может быть получена в форме: расширенных сообщений, выписки по счету, и т.п.);

10.1.6. другие события и обстоятельства, создающие угрозу использования Системы без согласия Клиента.

10.2. В случае наступления События компрометации или при наличии вероятности его наступления Клиент должен немедленно уведомить об этом Банк в порядке, установленном Соглашением. Письменное уведомление о Событии компрометации составляется по форме, установленной настоящими Правилами (Приложение № № 4).

10.3. При получении уведомления от Клиента о Событии компрометации по телефону Банк выполняет попытку проверки достоверности полученной информации путем звонка Клиенту:

10.3.1. на номер телефона, указанный в Заявке в качестве контактного;

10.3.2. на номера телефонов, используемых Клиентом для получения SMS-сообщений (за исключением случаев, когда соответствующее устройство утеряно/стало доступным для использования третьим лицам);

10.3.3. на другие номера телефонов, полученных от Клиента до наступления События компрометации (например, при открытии расчетного счета).

10.4. Банк обеспечивает невозможность совершения Операций ЭСП указанным в уведомлении о Событии компрометации Пользователем/Владельцем СКП и/или невозможность использования в Системе для совершения Операций ЭСП указанных в уведомлении о Событии компрометации номеров телефонов беспроводной (мобильной) связи:

10.4.1. в случае положительного результата проверки достоверности информации о наступлении События компрометации (согласно п. 10.3) и получения подтверждения События компрометации – на срок до 30 (тридцати) календарных дней;

10.4.2. в случае отрицательного результата проверки достоверности информации о наступлении События компрометации (согласно п. 6.3) - на срок до 2 (двух) рабочих дней, либо, в зависимости от полученных инструкций Клиента, не принимает мер, изложенных в п. 10.4 настоящих Правил.

10.5. При получении от Клиента письменного уведомления о Событии компрометации Банк обеспечивает применение мер, указанных в п. 10.4 настоящих Правил на неограниченный срок.

10.6. Для восстановления возможности работы в Системе Владельца СКП скомпрометированного ключа ЭП/номеров телефонов мобильной (беспроводной) связи, Клиент обращается в Банк с новой Заявкой.

11. Требования по обеспечению безопасности

11.1. Работа с паролями и кодами:

11.1.1. многоразовые пароли, создаваемые Клиентом самостоятельно не должны быть простыми. Рекомендуется составлять пароли длиной не менее 8-ми символов, состоящие из прописных и строчных букв (A-Z, a-z), цифр (0-9) и специальных символов (-!@#$~?). Не рекомендуется использовать имена и фамилии друзей и родственников, даты рождения, части Логинов Пользователя;

11.1.2. пароли и коды необходимо сохранять в тайне. Категорически воспрещается записывать и оставлять пароли и коды в доступном месте, а также передавать пароли и коды третьим лицам;

11.1.3. запрещается использовать на компьютере функцию автоматического сохранения паролей;

11.1.4. пароли необходимо менять. Рекомендуется не менее одного раза в 60 дней менять все многоразовые пароли, используемые в Системе «Электронный Банк», а при возникновении подозрений о возможной компрометации пароля его следует заменить немедленно.

11.2. Работа с ключами ЭП:

11.2.1. запрещается передавать любым третьим лицам свои ключи ЭП;

11.2.2. запрещается копировать ключи ЭП на жесткий диск или в системный реестр компьютера;

11.2.3. носитель ключа должен быть подключен к компьютеру (вставлен в компьютер) только во время работы с Системой. Во всех остальных случаях носитель ключа должен быть отключен от компьютера и храниться в недоступном для посторонних лиц месте;

11.2.4. ключи ЭП должны быть защищены сложными паролями, которые должны регулярно меняться;

11.2.5. в целях снижения рисков несанкционированного копирования ключей ЭП рекомендуется применять защищенные носители (электронный ключ e-token).

11.3. Защита устройства, на котором установлено/настроено рабочее место Клиента «Электронный Банк» (в т.ч. мобильное приложение):

11.3.1. на устройстве следует использовать только программное обеспечение, на которое получена лицензия в порядке, установленном ее правообладателем. Рекомендуется устанавливать программы, полученные только из доверенных источников – приобретенные у официальных поставщиков или загруженные с официальных Интернет-ресурсов;

11.3.2. не рекомендуется устанавливать программное обеспечение, которое не требуется для использования Системы;

11.3.3. не следует выполнять операции, не связанные с использованием Системы, особенно: прием и отправку электронной почты, просмотр Интернет-сайтов, загрузку файлов из сети Интернет, открытие файлов, находящихся на съемных носителях (флэш-накопители, внешние жесткие диски и т.п.);

11.3.4. необходимо на постоянной основе отслеживать выпуск и незамедлительно устанавливать последние обновления от разработчиков операционной системы устройства и Интернет-обозревателя, особенно «критические» обновления и обновления безопасности;

11.3.5. на компьютере (за исключением смартфонов) должен быть включен и настроен межсетевой экран (брэндмауэр);

11.3.6. на устройствах должно быть установлено, регулярно обновляться и функционировать антивирусное программное обеспечение;

11.3.7. использование средств удаленного управления компьютером допускается только в случаях и в порядке, предусмотренном п. 13 настоящих Правил. Во всех прочих случаях запрещается устанавливать на компьютер, используемый для работы с Системой, средства удаленного управления компьютером. На компьютере, используемом для работы в Системе, рекомендуется отключить встроенные в операционную систему возможности удаленного доступа «Удаленный помощник» и «Удаленный рабочий стол».

11.3.8. на Мобильном устройстве должна использоваться парольная защита;

11.3.9. окончание работы с Мобильным приложением должно осуществляться через завершение сессии («Выход»);

11.3.10. запрещается отключение встроенных защитных механизмов операционной системы Мобильного устройства путем взлома (Jailbreak). Jailbreak делает Мобильное устройство уязвимым к заражению вирусным ПО;

11.3.11. при потере Мобильного устройства необходимо обратиться в Банк для блокировки в Системе номера телефона и запрета доступа к Мобильному приложению;

11.3.12. запрещено переходить по ссылкам и устанавливать приложения/обновления безопасности, пришедшие по SMS/электронной почте, в том числе от имени Банка;

11.3.13. не рекомендуется работа с Системой с гостевых рабочих мест (интернет-кафе и т.п.) и с использованием общественных сетей Wi-Fi. Это связано с повышенными рисками хищения и дальнейшего неправомерного использования паролей и сеансовых ключей.

11.4. Дополнительные организационные меры обеспечения безопасности:

11.4.1. в организации Клиента соответствующими приказами следует назначить Владельцев СКП - пользователей СКЗИ и должностных лиц, ответственных за обеспечение безопасности информации и эксплуатации СКЗИ;

11.4.2. рекомендуется разработать внутренние нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ;

11.4.3. рекомендуется организовать поэкземплярный учет носителей ключевой информации с их хранением в сейфе или ином хранилище, обеспечивающем сохранность ключевой информации в отсутствие Владельца СКП.

12. Установка и настройка рабочего места Клиента

12.1. Установка и настройка рабочего места Клиента Системы может быть выполнена Клиентом самостоятельно или, по запросу Клиента, - силами Банка (путем выезда сотрудника/представителя Банка к Клиенту. Представителем Банка может быть в т.ч. третье лицо, действующее на основании договора/доверенности). В обоих случаях установка должна выполняться на рабочие места, соответствующие требованиям, установленным Приложением № № 3 к настоящим Правилам.

13. Удаленный доступ к компьютеру Клиента

13.1. При самостоятельной установке рабочего места Системы и при дальнейшем использовании Системы Клиент имеет право получить помощь Банка по вопросам установки, настройки и эксплуатации, в том числе путем временного предоставления сотруднику/представителю Банка удаленного доступа к компьютеру, на котором осуществляется работа с Системой.

13.2. Удаленный доступ предоставляется при помощи программы TeamviewerQS (http://www.teamviewer.com), которая обеспечивает:

13.2.1. полное шифрование данных;

13.2.2. генерирование идентификатора (ID) и пароля сеанса, который меняется при каждом запуске программы;

13.2.3. невозможность незаметного удаленного управления компьютером (путем индикации пользователю компьютера информации о попытках получения удаленного доступа к компьютеру).

13.3. Удаленный доступ осуществляется в следующем порядке:

13.3.1. Клиент получает программу TeamViewerQS из Банка по электронной почте, или на сменном носителе информации, либо путем загрузки с Интернет-сайта Банка;

13.3.2. Клиент запускает программу TeamViewerQS на компьютере, к которому должно быть выполнено удаленное подключение;

13.3.3. Клиент направляет в Банк письменный запрос об удаленном подключении к его компьютеру. Запрос направляется в произвольной форме по электронной почте, через Интернет-сайт Банка или через Систему. Запрос должен содержать название Клиента и его ИНН, а также идентификатор (ID), полученный Клиентом при помощи программы TeamViewerQS;

13.3.4. Клиент сообщает по телефону в Банк о направленном запросе, подтверждает указанную в нём информацию, в том числе идентификатор (ID), и сообщает пароль, полученный при помощи программы TeamviewerQS. Телефонный разговор Клиента с Банком записывается Банком;

13.3.5. сотрудник Банка с помощью программы TeamViewerQS подключается к компьютеру Клиента и выполняет на нем действия, необходимые для обеспечения работы Системы. Во время осуществления работ Клиент имеет возможность голосовой связи по телефону с сотрудником Банка, осуществляющим работы на компьютере Клиента;

13.3.6. Клиент получает по телефону информацию о том, что проведение работ на компьютере завершено и закрывает программу TeamViewerQS.

13.4. Клиент обязуется не использовать программное обеспечение TeamViewerQS, предоставленное Банком, в иных целях, кроме указанных в настоящих Правилах;

13.5. Клиент обязан сохранять в тайне идентификатор (ID) и пароль, полученные при помощи программы TeamViewerQS, и несёт ответственность за обеспечение недоступности этих данных для третьих лиц. Клиент осведомлен о возможности получения удаленного доступа к компьютеру Клиента третьими лицами при ненадлежащей защите Клиентом идентификатора (ID) и пароля. Клиент подтверждает, что все работы сотрудника Банка контролируются Клиентом визуально и/или посредством голосовой связи. Клиент обязуется самостоятельно обеспечить безопасность своего компьютера согласно рекомендациям Банка. В случае возникновения подозрения на наличие несанкционированного доступа к компьютеру Клиента с помощью программы TeamViewerQS, Клиент обязан максимально быстро разорвать подозрительное соединение и обратиться в Банк.

14. Проверка подлинности Электронной Подписи при урегулировании разногласий

14.1. Проверка подлинности Усиленной Электронной Подписи осуществляется в следующем порядке:

14.1.1. Банк предъявляет действовавший на момент подписания ЭД Сертификат ключа проверки электронной подписи Клиента.

14.1.2. Проверка ЭП выполняется путем использования: сообщения, содержащего оспариваемый Электронный документ; Сертификата ключа проверки электронной подписи и АРМ РКС «КриптоПро».

14.1.3. Результатом проверки является отчет, выдаваемый АРМ РКС .

14.1.4. Заключение о подлинности Электронной подписи делается на основании наличия или отсутствия соответствующего подтверждения подлинности

Электронной подписи (например, «Электронная подпись – ВЕРНА») в отчете, выданном АРМ РКС .

14.1.5. По требованию Клиента может быть проверена принадлежность предъявленного электронного Сертификата Клиенту (конкретному Владельцу СКП). Условия, определяющие принадлежность Сертификата Клиенту устанавливаются п.п. 3.9 и 3.10.

14.2. Проверка подлинности Простой Электронной Подписи PayControl:

14.2.1. Банк предоставляет:

14.2.1.1. идентификатор пользователя;
14.2.1.2. файл спорного электронного документа и/или данные транзакции;
14.2.1.3. ЭП, выработанную на ассиметричных ключах или код подтверждения, выработанный на симметричных ключах;
14.2.1.4. время выработки ЭП.

14.2.2. Данные, перечисленные в п. 14.2.1 загружаются в АРМ РКС «СейфТек».

14.2.3. Заключение о подлинности Электронной подписи делается на основании наличия или отсутствия соответствующего подтверждения подлинности Электронной подписи (например, «Verified successfully») в отчете, выданном АРМ РКС.

14.2.4. По требованию Клиента дополнительно может быть проверена принадлежность ПЭП конкретному Владельцу ключа (путем проверки выполнения условий 4.3.7 или 4.4.6).

14.3. Проверка подлинности Простой Электронной Подписи OTP осуществляется:

14.3.1. По инструкциям, предоставляемым организацией-разработчиком программного обеспечения, используемого в Системе (Разработчик).

14.3.2. При проверках используются средства, данные и электронные журналы Системы, программные средства и алгоритмы, рекомендуемые Разработчиком, а также документы, оформленные в целях обслуживания Клиента в Банке.

Приложение № 1 Форма Акта признания ключа

АКТ ПРИЗНАНИЯ ОТКРЫТОГО КЛЮЧА ЭП (СЕРТИФИКАТА) ДЛЯ ОБМЕНА СООБЩЕНИЯМИ	
Настоящим Актом признается ключ шифрования, принадлежащий уполномоченному представителю:	
ФИО владельца сертификата:	
Организация:	
Ключ ЭП создан с использованием СКЗИ:	
Идентификатор ключа:	
Хранилище ключевой информации:	
Момент генерации ключа:	
Открытый ключ клиента:	
Достоверность приведенных данных подтверждаем:	
От Банка _____/_____/	Индивидуальный предприниматель/единоличный исполнительный орган Клиента _____/_____/

Приложение № 2 Форма Доверенности на полномочного представителя

Доверенность на полномочного представителя

г. _____ " _____ " _____ 20___ г.

(место выдачи)

_____, далее – Клиент,

(полное наименование организации или ФИО индивидуального предпринимателя, ИНН/ОКПО Клиента)

Внимание! Секция "в лице" применима только для юридических лиц, для ИП не применима:

в лице _____,

(должность, фамилия, имя, отчество единоличного исполнительного органа Клиента)

действующего на основании Устава,

уполномочивает _____

(должность, фамилия, имя, отчество полномочного представителя)

- паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи;
- телефон для связи,

от имени Клиента использовать Систему «Электронный Банк» для целей осуществления операций по банковским счетам Клиента, открытым в АО «Банк Интеза» («Банк»), получения Банковской информации (как она определена в Соглашении об обслуживании в Системе «Электронный Банк Digitale» («Соглашение»), заключенном с Клиентом, представления интересов Клиента перед Банком по вопросам исполнения заключенных договоров банковского счета, осуществления обмена информацией и документами, необходимыми для совершения операций по банковским счетам Клиента в Банке и получения прочих услуг, предусмотренных Соглашением, со следующими полномочиями:

☐ Группа А;
☐ Группа Б;
☐ Техническая подпись;
☐ Особая подпись.

Содержание полномочий для случая «Особая подпись»:

Лицо, наделенное полномочиями Группы А, помимо указанного выше вправе от имени Клиента посредством Системы «Электронный Банк» заключать с Банком договоры/соглашения/сделки, определенные как «ЭД типа соглашение/сделка», в том числе открывать счета (включая депозитные), а также совершать иные фактические и юридические действия, необходимые для выполнения данного поручения.

Настоящая доверенность действительна до "_____" _____ 20___ года.

Настоящая доверенность выдана без права передоверия.

Клиент

_____/ _____/

М.П.

Приложение № 3 Требования к аппаратному и программному обеспечению рабочего места Клиента

Рабочее место Подсистемы «Интернет-Клиент»:

СКЗИ: КриптоПро CSP 4.0.

Аппаратная часть рабочего места:

- IBM-совместимый компьютер с CPU 1.6 ГГц (Intel Pentium / Celeron или AMD), ОЗУ 1 Гб, сетевой платой Ethernet 100 Мбит/сек, манипулятором "мышь", разрешение экрана 1024x728 пикселей, не менее 100 Мб свободного места на жестком диске.
- Устойчивое соединение с сетью Интернет по протоколу HTTPS.
- Порт USB 2.0.
- Для работы с Усиленной Электронной Подписью - eToken PRO либо иной носитель ключа, совместимый с КриптоПро CSP 4.0 (см. https://www.cryptopro.ru/products/csp/compare). На Mac OS требуется использование носителя ключа Рутокен ЭЦП 2.0.
- Допускается использование средства визуализации подписываемых данных SafeTouch PRO (при одновременном использовании носителя ключа Рутокен ЭЦП 2.0).

Операционные системы:

- Windows 7; 8 x86/x64; Windows 8.1 x86/x64; Windows 10.
- Windows Server 2003 R2 x64; 2008 x86, x64; 2008 R2; 2012; 2012 R2.
- Mac OS 10.9.5 Mavericks, 10.13.1, 10.13.2.

Интернет браузеры для стационарных компьютеров и ноутбуков, в зависимости от используемой ОС:

	Windows				Windows Server				macOS		
Браузер	7	8	8.1	10	2003 R2 x64	2008 x86, x64; 2008 R2	2012	2012 R2	10.9.5 Mavericks	10.13.1	10.13.2
Edge				+ a							
Chrome 47 и выше	+	+	+	+	+	+	+	+			
Firefox 44.0 и выше	+	+		+	+						
Internet Explorer 10	+	+				+ b	+				
Internet Explorer 11	+		+	+		+ b		+			
Opera 36 и выше	+	+	+	+	+	+	+	+			
Safari 9 и выше									+	+	+

a - Без поддержки использования СКЗИ
b - Только 64-разрядная версия Windows Server 2008 R2 с пакетом обновления 1 (SP1)

Дополнительное ПО:

- Microsoft Excel - 2007, 2010, 2013, Office:Mac 2011.
- Adobe Acrobat Reader - 9.0 и выше.
- Microsoft Word - 2007, 2010, 2013, Office:Mac 2011.

Рабочее место Подсистемы «Мобильный Клиент»:

Операционные системы:

- Android 5.0 и выше.
- iOS 10.X, 11.X.

Приложение № 4 Форма Уведомления о Событии компрометации

В АО «Банк Интеза»

Уведомление о Событии компрометации

В Системе «Электронный Банк»

" _____ " _____ 201_ г.

Наименование организации: _____

ИНН/ОКПО:_____

В лице _____,

действующего на основании _____,

настоящим уведомляет о следующем событии:

☐ скомпрометированы ключи, Владелец ключей:

ФИО:_____

Номер носителя ключа (если известен): _____

☐ обнаружены расходные операции, которые были совершены без нашего согласия:

сумма _____

дата _____

номер документа_____

получатель_____

☐ иное событие (указать):

Краткое описание события и обстоятельств:

Телефонное обращение в Банк в связи с указанным событием/обстоятельствами:

☐ было выполнено _____(дата, московское время), со следующего номера телефона _____.

☐ не выполнялось;

☐ неизвестно (информация по телефонному сообщению отсутствует).

дата _____ /_____/