

## Правила использования Системы «Электронный Банк Digitale»

### Оглавление

1. Термины .....	2
2. Пользователи и их полномочия в Системе .....	4
3. Усиленная Электронная Подпись .....	5
4. Одноразовый Пароль.....	6
5. Простая Электронная Подпись.....	6
6. Подсистема «Интернет-Клиент» .....	6
7. Подсистема «Мобильный Клиент».....	9
8. Сообщения: SMS, PUSH и e-mail .....	11
9. Дополнительное подтверждение Электронного Документа.....	12
10. События компрометации.....	13
11. Требования по обеспечению безопасности .....	14
12. Установка и настройка рабочего места Клиента .....	16
13. Удаленный доступ к компьютеру Клиента.....	16
14. Проверка подлинности Электронной Подписи при урегулировании разногласий .....	17
Приложение 1 Форма Акта признания ключа .....	19
Приложение 2 Форма Доверенности на полномочного представителя.....	20
Приложение 3 Требования к аппаратному и программному обеспечению рабочего места Клиента	21
Приложение 4 Форма Уведомления о Событии компрометации .....	22
Приложение 5 Форма Акта об оказании услуг по установке и настройке программного обеспечения Системы .....	23

## 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** – это персональное сообщение Пользователю, направляемое ему через Подсистему «Мобильный Клиент».
- 1.2. **Акт признания ключа** – документ на бумажном носителе по форме, установленной Приложением 1 к настоящим Правилам, который может быть использован для установления принадлежности ключа (СКП) УЭП конкретному Владельцу СКП.
- 1.3. **Владелец Сертификата ключа проверки электронной подписи (Владелец СКП)** – Пользователь, на имя которого ЦУС выдал СКП и который владеет соответствующим ключом Усиленной Электронной Подписи.
- 1.4. **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», Электронные документы подписываются одной подписью любым Пользователем, отнесенным к «Группе А».
- 1.5. **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». Электронные документы подписываются двумя подписями. При этом одна подпись должна принадлежать «Группе А», а другая - «Группе Б».
- 1.6. **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).
- 1.7. **Заявка** - заявка на установку параметров подключения к системе «Электронный Банк Digitale» (Приложение №2<sup>Б</sup> к Соглашению).
- 1.8. **Логин Пользователя** – уникальный универсальный идентификатор Пользователя в Подсистемах. Логин Пользователя назначается при подключении к Системе «Электронный Банк Digitale», либо может быть унаследован при Миграции из Системы «Электронный Банк transact». Разрешается самостоятельная замена логина Пользователем средствами Системы.
- 1.9. **Особая подпись** – категория, определяющая право подписи Пользователя в Системе и/или применяемый порядок использования Электронной Подписи в Системе. 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 прав Особой подписи в каждом конкретном случае оговаривается Банком и Клиентом в Заявке на установку

параметров подключения к системе «Электронный Банк Digitale» (Приложение №2<sup>Б</sup> к Соглашению).

- 1.10. **Перечень Допустимых Получателей (ПДП)** - перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием Системы. При использовании Клиентом ПДП в адрес получателей, не входящих в ПДП, переводы денежных средств с использованием Системы совершены быть не могут.
- 1.11. **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:
  - 1.11.1. для Подсистемы «Интернет-Клиент»: IP-адрес и MAC-адрес;
  - 1.11.2. для Подсистемы «Мобильный Клиент»: Pseudo-Unique ID (для мобильных устройств на базе Android) и Identifier for Vendor (IDFV, для iPhone).
- 1.12. **Простая Электронная Подпись (ПЭП)** - Электронная подпись, которая посредством использования комбинации кодов, паролей или иных средств однозначно подтверждает факт авторства подписанного документа определенного лица (Клиента, Пользователя).
- 1.13. **Сертификат ключа проверки электронной подписи (СКП, Сертификат)** – Электронный документ с Электронной подписью уполномоченного лица ЦУС, который включает в себя ключ проверки Усиленной Электронной Подписи и который выдается ЦУС и используется для подтверждения подлинности Электронной подписи и идентификации Владельца Сертификата ключа проверки электронной подписи.
- 1.14. **Средства криптографической защиты информации (СКЗИ)** – Средства электронной подписи, обеспечивающие работу с Усиленной Электронной Подписью. В Системе «Электронный Банк» используются СКЗИ: "КриптоПро CSP", а также «АРМ разбора конфликтных ситуаций», разработанные ООО «КРИПТО-ПРО».
- 1.15. **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.
- 1.16. **Техническая подпись** – категория, определяющая право подписи в Системе. При предоставлении полномочий «Техническая подпись» обеспечивается работа Пользователя с выписками и ЭД без права их подписи.
- 1.17. **Усиленная Электронная Подпись (УЭП)** - реквизит Электронного документа, предназначенный для защиты данного Электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием ключа Электронной подписи и позволяющий идентифицировать Владельца Сертификата ключа проверки электронной подписи, а также установить отсутствие искажения информации в Электронном документе. В Системе «Электронный Банк» используются Усиленные Электронные Подписи, которые в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи» являются неквалифицированными.

- 1.18. **Центр управления сертификатами (ЦУС)** – организационно–техническая система управления ключевой информацией Системы, включающая в себя:
- 1.18.1. персонал Банка, осуществляющий эксплуатацию и обеспечивающий работоспособность и информационную безопасность ЦУС;
  - 1.18.2. программно-аппаратное обеспечение ЦУС;
  - 1.18.3. 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. При Миграции список Пользователей и их полномочия наследуются из Системы «Электронный Банк transact».
- 2.4. Для изменения содержания прав действующих Пользователей Клиент предоставляет в Банк документы, указанные в п.п. 2.2.1, 2.2.2.
- 2.5. В случае изменения списка Пользователей Клиент представляет в Банк новую Заявку.
- 2.6. 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.
- 2.7. 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.
- 2.8. Если заблаговременная подача Заявки, документов, подтверждающих изменения полномочий, невозможна, в отношении Пользователей, полномочия которых прекращены/ограничены, Клиент дополнительно применяет порядок действий, установленный п.9.

### 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, Очередным или Унаследованным.
- 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.
- 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. Подпись запроса на СКП Унаследованным ключом не допускается.
- 3.7. Унаследованный ключ (и соответствующий ему СКП) – это ключ (СКП), созданный в Системе «Электронный Банк transact» по правилам Системы «Электронный Банк transact». Использование Унаследованного ключа (СКП) допускается после Миграции до истечения срока действия Унаследованного ключа. Для дальнейшей работы в Системе Клиент должен создать Первый ключ в соответствии с п.3.5.
- 3.8. Банк выпускает Клиенту СКП на основании запроса на СКП, полученного по Системе.
- 3.9. Банк разрешает использование Клиентом Первого ключа только при условии предоставления Клиентом в Банк оригинала Акта признания ключей.
- 3.10. Первый СКП признается принадлежащим конкретному Владельцу СКП, если запрос, на основании которого выпущен Первый СКП, подписан ключом, указанным в Акте признания ключей.
- 3.11. Очередной СКП признается принадлежащим конкретному Владельцу СКП, если:
  - 3.11.1. в соответствии с п. 3.10 установлена принадлежность Первого СКП данному Владельцу СКП;
  - 3.11.2. 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.
- 3.12. Признание принадлежности Унаследованного СКП конкретному Владельцу СКП осуществляется по правилам Системы «Электронный Банк transact».
- 3.13. Срок действия ключа (Первого, Очередного, Унаследованного) и соответствующего ему СКП указывается в СКП.

- 3.14. Применяемые в Системе «Электронный Банк» СКЗИ и 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.
- 3.15. 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. Одноразовый Пароль

- 4.1. Одноразовый пароль – это последовательность символов, которая направляется Клиенту (Пользователю) в автоматическом режиме в форме SMS-сообщения на номер, указанный Клиентом согласно п.8.1.1, либо в форме PUSH-сообщения (п.п.7.6, 8.3).
- 4.2. Одноразовый пароль имеет ограниченный срок действия, который устанавливается Банком.

#### 5. Простая Электронная Подпись

- 5.1. ПЭП проставляется путем ввода Клиентом в Систему одноразового пароля для конкретного ЭД.
- 5.2. В случае использования Клиентом ПЭП Банк имеет право в целях управления рисками ограничивать суммы Электронных Платежных Документов.

#### 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 УЭП/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 (в том числе, с прикрепленными документами);
  - 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 (в том числе, с прикрепленными документами);
  - 6.2.8. справка о подтверждающих документах (в том числе, с прикрепленными документами);
  - 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. письма в свободном формате (в том числе, с прикрепленными документами), за исключением документов, связанных с продлением полномочий Пользователей, внесением изменений в карточку с образцами подписей и оттиска печати и уставные документы, заключением или расторжением договоров на предоставление банковских услуг (если это не предусмотрено отдельным соглашением Сторон), а также изменением иных данных Клиента, имеющих в Банке.
  - 6.2.15. Запрос на отзыв платежного поручения.
- 6.3. При использовании ПЭП принимаются в обработку следующие типы Электронных документов:
- 6.3.1. Заявление на перевод в рублях.
  - 6.3.2. Запрос на отзыв платежного поручения.
- 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. Многоцветные 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.
    - 6.5.1.5. В случае Миграции пароль интернет-пользователя наследуется из Системы «Электронный Банк transact».
  - 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. Для Унаследованного ключа пароль к носителю ключа/ к контейнеру с ключом ЭП сохраняется таким же, каким он был при использовании ключа в Системе «Электронный Банк transact».

- 6.5.2.4. 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.
- 6.5.2.5. 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» либо после Миграции, либо 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;
- 6.6.7. в целях обеспечения возможности использования УЭП осуществляется:
- 6.6.7.1. создание Клиентом ключей УЭП;
- 6.6.7.2. оформление Клиентом и передача в Банк Акта признания ключей (Приложение 1 к настоящим Правилам);
- 6.6.7.3. выпуск Банком Сертификата ключа проверки электронной подписи (СКП);
- 6.6.7.4. ввод СКП в действие после проверки Банком Акта признания ключей.
- 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:
- 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 «четыре глаза» 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 смартфоне Клиента (iPhone, смартфоны под управлением операционной системы Android) при применении Простой Электронной Подписи.

- 7.2. Для получения обслуживания в полном объеме, в частности, для использования функций, перечисленных в п.п. 7.9, 7.10 и 7.11, 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.
- 7.4. 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 смартфоном 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. PUSH-сообщения.
- 7.6.1. Содержание PUSH-сообщения отображается Пользователю с использованием мобильного приложения подсистемы «Мобильный Клиент» после предъявления Пользователем кодов/паролей, а также использования биометрических средств аутентификации согласно п.7.5.
- 7.7. Клиент допускается к работе с Подсистемой «Мобильный Клиент» либо после Миграции, либо после выполнения им всей совокупности следующих действий:
- 7.7.1. ознакомление с условиями Соглашения и настоящих Правил;
- 7.7.2. оформление Заявки;
- 7.7.3. подтверждение права Электронной Подписи Пользователей в соответствии с п. 2.2;
- 7.7.4. подготовка рабочего места в соответствии с требованиями Приложения 3 к настоящим Правилам;
- 7.7.5. получение сообщения из Банка о готовности банковской части Системы к обслуживанию Клиента в Системе;
- 7.7.6. скачивание Клиентом из репозиторий Apple Store/Play Market мобильного приложения [bancaintesadigitale](https://www.bancaintesadigitale.it) и установка его на смартфон Клиента.
- 7.8. Ограничение максимальной суммы переводов денежных средств:

- 7.8.1. В целях ограничения рисков Банк устанавливает суточный лимит на максимально допустимую сумму ЭПД Клиента, подписанных Простой Электронной Подписью с использованием Подсистемы «Мобильный Клиент». Банк не принимает в обработку Электронные Платежные Документы в случае, если их сумма превышает установленный суточный лимит. Значения установленных суточных лимитов отображаются Клиенту с использованием Подсистемы «Мобильный Клиент».
- 7.8.2. Клиент вправе установить в порядке, определенном в п.6.8, дополнительные ограничения на максимальные суммы переводов денежных средств.
- 7.9. Уведомления об Операциях ЭСП, совершенных с использованием Подсистемы «Мобильный Клиент», направляются через Подсистему «Интернет-Клиент» по правилам, указанным в п.6.7.
- 7.10. Использование Перечня Допустимых Получателей (ПДП) осуществляется по правилам, указанным в п.6.9. При этом самостоятельное формирование Клиентом ПДП выполняется в Подсистеме «Интернет-Клиент».
- 7.11. Использование Перечня Идентификаторов Допустимых Устройств (ПИДУ) и Допустимого Временного Периода (ДВП) осуществляется согласно п. 6.10.

## 8. Сообщения: SMS, PUSH 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;
- 8.1.1.3. унаследованные для конкретного Клиента из Системы «Электронный Банк transact» в результате Миграции.

#### 8.1.2. SMS сообщения могут использоваться для дублирования PUSH-сообщений согласно п. 8.3.3.

### 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.

### 8.3. Получатель PUSH-сообщения. Дублирование PUSH-сообщений.

#### 8.3.1. Банк направляет PUSH-сообщения при наличии технической возможности.

#### 8.3.2. Получателем PUSH-сообщения является Пользователь подсистемы «Мобильный Клиент» (см. п.7.6).

#### 8.3.3. Пользователям Подсистемы «Мобильный Клиент» сообщения, которые могут быть направлены в форме PUSH или SMS:

- 8.3.3.1. направляются в форме PUSH;
- 8.3.3.2. в случае невозможности доставки сообщения, отправленного согласно п. 8.3.3.1, оно дублируется в форме SMS.

#### 8.4. Базовые сообщения.

- 8.4.1. Базовыми являются сообщения, необходимые для использования Клиентом Системы.
- 8.4.2. Базовые сообщения направляются Клиенту без взимания дополнительной платы.
- 8.4.3. Базовые сообщения используются для отправки Клиенту:
  - 8.4.3.1. Логина Пользователя посредством e-mail (п.1.8);
  - 8.4.3.2. пароля Интернет-пользователя посредством SMS (п.п.6.5.1, 7.5.1);
  - 8.4.3.3. одноразовых паролей посредством SMS/PUSH;
  - 8.4.3.4. номера лицензии СКЗИ посредством SMS/e-mail;
  - 8.4.3.5. инструкций по установке, настройке и использованию Системы посредством e-mail.

#### 8.5. Расширенные сообщения.

- 8.5.1. Расширенными являются сообщения, которые не являются необходимыми для использования Клиентом Системы.
- 8.5.2. Расширенные сообщения используются для предоставления Клиенту оперативной информации о событиях, связанных с Системой.
- 8.5.3. Банк может устанавливать в Тарифах и взимать плату за предоставление расширенных сообщений.

#### 8.6. Ограничение ответственности Банка в отношении SMS, PUSH и e-mail.

- 8.6.1. В соответствии с настоящими Правилами Клиент предоставляет Банку право направлять информацию, указанную в п.8. Правил, посредством отправки SMS, PUSH и e-mail.
- 8.6.2. Банк обеспечивает возможность настройки параметров расширенных сообщений (п.8.5), в том числе выбор из списка событий, в отношении которых отправляются сообщения, и настройку параметров для отправки таких сообщений.
- 8.6.3. Клиент обязуется принимать достаточные и необходимые меры для защиты информации, отправляемой путем SMS, PUSH и e-mail, и ограничения доступа к такой информации неуполномоченных лиц.
- 8.6.4. Клиент освобождает Банк от ответственности за ненадлежащее исполнение обязательств в части отправки SMS, PUSH 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 одноразового пароля.
- 9.2. Если для конкретного Электронного документа запрошено дополнительное подтверждение, Банк имеет право не проводить обработку этого документа до момента ввода Клиентом в Систему соответствующего одноразового пароля.

## 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/PUSH-сообщений;

10.1.3. случаи, когда устройство, обеспечивающее прием SMS/PUSH-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 только полученные 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 (брандмауэр);
  - 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 (Jailbreake). Jailbreake 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.
- 12.2. Факт установки Системы у Клиента силами Банка оформляется Актом об оказании услуг по установке и настройке программного обеспечения Системы, который подписывается Сторонами (Приложение 5 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 СКЗИ («АРМ разбора конфликтных ситуаций»).

14.1.3. Результатом проверки является отчет, выдаваемый «АРМ разбора конфликтных ситуаций».

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 разбора конфликтных ситуаций».

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. 3.10, 3.11 и 3.12.

14.2. Проверка подлинности Простой Электронной Подписи осуществляется:

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

14.2.2. 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

<b>АКТ ПРИЗНАНИЯ ОТКРЫТОГО КЛЮЧА ЭП (СЕРТИФИКАТА)                      ДЛЯ ОБМЕНА СООБЩЕНИЯМИ</b>	
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», представления интересов Клиента перед АО «Банк Интеза» по вопросам исполнения заключенных договоров банковского счета, осуществления обмена информацией и документами, необходимыми для совершения операций по банковским счетам Клиента в АО «Банк Интеза» со следующими полномочиями:

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

Содержание полномочий для случая «Особая подпись»:

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.

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:

Браузер	Windows				Windows Server				macOS		
	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 \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Приложение 5      Форма Акта об оказании услуг по установке и настройке программного обеспечения Системы

Акт об оказании услуг по установке и настройке программного обеспечения «Электронный Банк»

Г. \_\_\_\_\_  
(место составления)

" \_\_\_\_ " \_\_\_\_\_ 201\_\_ г.

Мы, \_\_\_\_\_, нижеподписавшиеся, уполномоченный представитель \_\_\_\_\_, далее – Клиент,  
(полное наименование организации Клиента)

в лице \_\_\_\_\_, действующего на основании \_\_\_\_\_,  
(должность, фамилия, имя, отчество)

\_\_\_\_\_, с одной стороны, и уполномоченный представитель АО «Банк Интеза», далее – Банк, в лице \_\_\_\_\_, действующего на основании \_\_\_\_\_,  
(должность, фамилия, имя, отчество)

\_\_\_\_\_, с другой стороны, составили настоящий акт о том, что уполномоченный представитель Банка оказал услуги, а уполномоченный представитель Клиента принял услуги по установке и настройке программного обеспечения «Электронный Банк». У сторон отсутствуют претензии по установке и настройке программного обеспечения «Электронный Банк».

Сумма оплаты услуг:

- Определяется тарифами Банка
- Установлена индивидуально в размере (указать сумму):

Настоящий Акт составлен в двух экземплярах – по одному экземпляру для каждой стороны.

От Клиента

\_\_\_\_\_  
(должность, фамилия, имя, отчество Уполномоченного лица)

\_\_\_\_\_  
(подпись Уполномоченного лица)

От Банка

\_\_\_\_\_  
(должность, фамилия, имя, отчество Уполномоченного лица)

\_\_\_\_\_  
(подпись Уполномоченного лица)