

Порядок управления ключами КА (ЭП) и ключами шифрования, применяемыми при формировании и передаче отчетности по форме 0409701, в рамках «Договора о передаче-приёме отчётности в виде электронных сообщений, снабженных кодом аутентификации»

### **Термины и определения.**

Администратор ключевой системы (далее - АКС) - должностное лицо Банка, основной обязанностью которого является управление ключевой системой: регистрация или сертификация ключей, формирование списка отозванных сертификатов, организация плановой смены ключей.

Ключ регистрации - закрытый криптографический ключ, сформированный Центром регистрации. Предназначен для создания закрытых ключей Клиента.

Ключевой носитель - отчуждаемый носитель, содержащий закрытый ключ.

Ключевая информация - совокупность используемых ключей.

Тестовая ключевая информация - ключевая информация, сформированная Банком и переданная Клиенту для организации взаимодействия со стендом совмещённого тестирования (далее - ССТ).

Центр Регистрации - управляющая компонента СКЗИ. Предназначен для регистрации ключей пользователей системы.

Центр управления ключевыми системами (далее - ЦУКС) - подразделение Банка, решающее задачи управления ключевой системой, регистрации и сертификации ключей.

## **1. Общие положения.**

1.1. Настоящий порядок описывает взаимодействие между Банком и Клиентом при работе с ключами КА (ЭП) и шифрования, применяемыми при формировании и передаче отчетности КО по форме 0409701

1.2. В ходе функционирования Клиентом должны формироваться и храниться в бумажном виде заверенная распечатка сертификата ключа Клиента.

## **2. Основные функции Банка и Клиента**

2.1. Основными функциями Банка являются следующие:

- регистрация и сертификация ключей Клиента;
- консультирование Клиента по вопросам регистрации и сертификации ключей;
- организация работ по плановой (или внеплановой) смене ключей Банка;
- формирование тестовых ключей для организации взаимодействия с ССТ.

2.2. Основными функциями Клиента являются следующие:

- ответственное хранение и защита от несанкционированного доступа к закрытому ключу;
- организация плановой (внеплановой) смены ключей Клиента;
- организация своевременной обработки файлов обновлений, поступающих из ЦУКС на соответствующих АРМ Клиента;
- комиссионное уничтожение выведенных из действия закрытых ключей с составлением акта;
- участие в рассмотрении спорных ситуаций между Клиентом и Банком.

### **3. Начало обслуживания и регистрация ключей Клиента.**

#### **3.1. Порядок формирования и получения тестовых ключей Клиента в ЦУКС.**

3.1.1. Тестовые ключи Клиента формируются в ЦУКС.

3.1.2. Тестовые ключи Клиента и справочники сертификатов передаются Клиенту в виде архивного файла.

3.1.3. Сертификаты СКАД «Сигнатура» тестовой серии ключей Банка, необходимые для организации взаимодействия с ССТ, в виде файлов обновлений размещены на официальном ресурсе Банка <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»)

3.1.4. При необходимости изготовления или плановой смены тестовых ключей, Клиент направляет в ЦУКС по электронной почте на адрес, указанный на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»), письмо-запрос, обязательно указав:

- в теме письма: **ТЕСТ\_701\_<краткое наименование организации>**,
- в тексте письма: наименование организации, БИК/УИС,

3.1.5. АКС не позднее чем через три рабочих дня после получения запроса передает Клиенту сформированные тестовые ключи и справочники сертификатов Клиента в виде архивного файла по электронной почте (на электронный адрес отправителя запроса).

#### **3.2. Порядок регистрации ключей в ЦУКС.**

Процедура регистрации ключей Клиента происходит по адресу и во время, указанные на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»).

Клиент обязан провести процедуру регистрации своих ключей при подключении, смене наименования/формы собственности, необходимости изготовления дополнительных ключей, неисправности ключевого носителя, истечении срока действия закрытого ключа.

### 3.2.1. Получение ключей и сертификатов регистрации Клиента в ЦУКС.

3.2.1.1. Клиент сдает в экспедицию Банка с сопроводительным письмом следующие документы:

1) Заявление на получение ключей и сертификатов регистрации, составленное в соответствии с образцом, (далее-Заявление).

#### Примечание:

- При формировании ключа регистрации поле сертификата ключа - *<наименование организации>* заполняется АКС в точном соответствии с наименованием (полным или сокращенным), указанным в Заявлении.

- Клиент указывает необходимые типы ключей и их количество. Рекомендуется: для обеспечения непрерывной и безотказной работы, изготавливать не менее чем по два ключа каждого типа.

#### Типы ключей для отправки формы 0409701:

- |                                  |   |
|----------------------------------|---|
| - Оператор подготовки            | -подпись (если для установки КА используется утилита SVK_PREPARE, а для шифрования используется АРМ КБР-Н); |
| - Оператор подготовки и отправки | -подпись и шифрование (для установки КА и шифрования используется утилита SVK_PREPARE)                      |

2) **Транспортный** съемный носитель для получения ключей и сертификатов регистрации (рекомендуется flash-drive). Съемный носитель должен быть отформатирован Клиентом и не должен содержать посторонней информации.

3.2.1.2. Не позднее чем через три рабочих дня после подачи Заявления Клиенту необходимо обратиться в ЦУКС по телефону, указанному на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»), для получения сведений о готовности ключевой информации.

3.2.1.3. За готовой ключевой информацией прибывает уполномоченный представитель Клиента, указанный в Заявлении. **При себе необходимо иметь паспорт.**

Выдача ключевой информации уполномоченному представителю Клиента производится в рабочие дни по адресу и во время, указанные на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/>.

3.2.1.4. Уполномоченный представитель Клиента получает:

- один экземпляр заверенной ЦУКС распечатки сертификата на каждый ключ регистрации Клиента;

- сертификат регистрации и ключ регистрации на предоставленных

ранее в качестве приложения к Заявлению съемных носителях.

Сертификат регистрации и ключ регистрации предназначены исключительно для формирования закрытого ключа и запроса на получение сертификата открытого ключа и, не могут быть использованы для отправки ЭС.

Ключ регистрации действителен один календарный месяц со дня его формирования, в течение этого месяца процедура регистрации закрытых ключей должна быть завершена.

3.2.1.5. Факт передачи ключа регистрации подтверждается проставлением даты получения и подписей уполномоченного представителя Клиента и АКС ЦУКС на каждой распечатке сертификата ключей регистрации Клиента. Один экземпляр распечатки сертификата на каждый ключ регистрации хранится в ЦУКС, второй экземпляр передается Клиенту.

### **3.2.2. Сертификация ключей Клиента.**

3.2.2.1. Сформированные запросы на получение сертификата Клиент передает в ЦУКС по электронной почте.

Для отправки запросов необходимо:

1) заархивировать запросы на получение сертификата– файлы \*.pse, в один файл с именем:

**Q\_<краткое наименование организации>.zip (.rar)**

(без создания папок);

2) отправить сформированный файл в ЦУКС по электронной почте на адрес, указанный на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»), обязательно указав в теме письма:

**701\_<краткое наименование организации>;**

3) уведомить ЦУКС по телефону, указанному на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»), об отправке запросов и получить подтверждение о приеме на сертификацию.

**Примечание:** Электронные письма с указанной темой должны содержать только запросы на получение сертификата (посторонняя информация удаляется автоматически).

Возможность несанкционированного изменения запроса на получение сертификата исключена, так как он формируется в формате упакованных данных с использованием электронной подписи на ключе регистрации Клиента или, в случае проведения плановой смены ключей, на действующем закрытом ключе Клиента.

В случае отсутствия электронной почты, съемный носитель с запросами на получение сертификата с сопроводительным письмом Клиент сдает в экспедицию Банка.

3.2.2.2. После получения запроса на получение сертификата АКС не позднее чем через пять рабочих дней формирует сертификат ключа.

3.2.2.3. Представитель Клиента получает в Банке по два экземпляра

распечатки сертификата на каждый ключ, заверенные подписями АКС и печатью ЦУКС.

3.2.2.4. Представитель Клиента доставляет в Банк **по два экземпляра распечатки сертификата на каждый ключ**, заверенные подписью (с расшифровкой фамилии) руководителя организации Клиента и печатью Клиента.

Факт передачи сертификата подтверждается проставлением даты получения штампа «получено в ЦУКС» и подписи АКС на каждой распечатке сертификата ключа Клиента. Один экземпляр оформленной распечатки сертификата на каждый ключ регистрации хранится в ЦУКС, второй экземпляр возвращается Клиенту.

3.2.2.5. АКС передает Клиенту сформированные сертификаты ключей Клиента в электронном виде по электронной почте (на электронный адрес отправителя запроса). Сертификаты передаются в виде файла обновлений (\*.pse).

В случае отсутствия у Клиента возможности получения файла обновлений по электронной почте АКС передает представителю Клиента сформированные сертификаты ключей на съемном носителе (предоставленном Клиентом) при личной явке.

#### **Внимание!**

- Получение Клиентом сертификатов ключей в электронном виде возможно **только после предоставления в ЦУКС оформленных распечаток сертификатов.**

- Сертификаты СКАД «Сигнатура» действующей серии ключей Банка, используемых при эксплуатации систем БЭСП и КОИ Банка России, в виде файлов обновлений выложены на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»).

## **4. Порядок смены ключей.**

4.1. В зависимости от типа выбранного ключевого носителя срок действия закрытых ключей при сертификации устанавливается равным: от одного года и трех месяцев до трёх лет.

4.2. **Смена ключа Клиента:** Клиент не менее чем за десять рабочих дней до окончания срока действия ключей, должен организовать плановую смену своих ключей: формирование новых закрытых ключей и отправку запросов на получение сертификатов в ЦУКС.

Порядок действий при сертификации новых ключей изложен в пп.3.2.2 настоящего Приложения.

4.3. **Смена ключа Банка:** Банк не позднее, чем за десять рабочих дней должен оповестить Клиента о сроке предстоящей плановой смене ключей Банка.

4.4. При получении письма и файла обновлений от Банка Клиент должен произвести обработку файла обновлений на всех АРМ в указанные сроки.

4.5. Клиент берет на себя полную ответственность и обязуется обеспечивать сохранность, неразглашение и нераспространение ключей неуполномоченным лицам. В том случае, если Клиент разрешает кому-либо использовать свои ключи, то он несет полную ответственность за соблюдение условий Договора, как со своей стороны, так и со Стороны, пользующейся его ключами.

## **5. Порядок действий в случае компрометации/досрочного прекращения срока действия закрытого ключа.**

Клиентом или Банком может быть принято решение о компрометации/досрочном прекращении срока действия своего закрытого ключа.

5.1. В случае принятия решения о компрометации закрытого ключа **использование скомпрометированного закрытого ключа должно быть прекращено.**

5.2. В случае принятия решения о компрометации/досрочном прекращении срока действия закрытого ключа Клиента, Клиент:

- организует формирование запроса на отзыв сертификата ключа;
- по электронной почте (или на съемном носителе) передает запрос в ЦУКС;
- сообщает в ЦУКС по телефону, указанному на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»), о компрометации/досрочном прекращении срока действия закрытого ключа и отправке запроса на отзыв сертификата.

При отправке запроса по электронной почте необходимо:

- заархивировать запрос на отзыв сертификата в файл с именем **Q\_<краткое наименование организации>\_отзыв.zip. (rar)** (без создания папок);
- отправить сформированный файл в ЦУКС по электронной почте на адрес, указанный на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»), обязательно указав в теме письма:

**701\_отзыв\_сертификата\_<краткое наименование организации>.**

При отсутствии возможности сформировать запрос на отзыв сертификата, передать в ЦУКС через экспедицию Банка «Уведомление о компрометации/досрочном прекращении срока действия закрытых ключей» (далее-Уведомление) в соответствии с образцом, размещенным на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»).

5.3. АКС, на основании запроса на отзыв сертификата ключа или Уведомления, формирует СОС, который содержит отзываемый сертификат.

Сертификат Клиента помещается в СОС с даты получения ЦУКС запроса на отзыв сертификата ключа или Уведомления.

СОС вступает в силу **не позднее** даты операционного дня, следующей

за датой отзыва сертификата.

По запросу Клиента, направленному в ЦУКС по электронной почте на адрес, указанный на официальном ресурсе Банка: <http://www.cbr.ru/mcirabis/> (раздел «Информация для клиентов Банка России при подключении к электронному обмену»), СОС может быть выслан Клиенту на адрес отправителя запроса или передан представителю Клиента на съемном носителе (предоставленном Клиентом) при личной явке.

5.4. При необходимости Клиент организует регистрацию нового ключа. Порядок действий при регистрации нового ключа изложен в пп.3.2.1 настоящего Приложения.

5.5. При компрометации закрытого ключа Банка АКС формирует новый СОС и направляет Клиенту информационное письмо и файл обновлений.

5.6. При получении информационного письма и файла обновлений от Банка Клиент должен произвести обработку файла обновлений на всех АРМ.