Регламент взаимодействия Банка России и Клиента при управлении криптографическими ключами,
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.

Термины, используемые в настоящем Регламенте, понимаются в значениях, установленных правилами платежной системы Банка России, документацией на СКАД «Сигнатура», а также Условиями по защите информации.

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 – криптографический ключ, предназначенный для создания криптографических ключей Клиента.

Ключевая информация – специальным образом организованная совокупность криптографических ключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Регистрационная карточка сертификата ключа регистрации – документ, содержащий распечатку сертификата ключа регистрации, включая распечатку в шестнадцатеричной системе счисления ключа, наименование и иные реквизиты, идентифицирующие владельца ключа, подпись АКС ЦУКС и печать ЦУКС.

Список отозванных сертификатов (далее – САС) – файл специального вида, содержащий имя Центра сертификации, выпустившего САС, дату выпуска, список элементов, каждый из которых включает ссылку на отзываемый сертификат и электронную подпись Центра сертификации, заверяющую совокупность этих данных.

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

Центр управления ключевыми системами Центра эксплуатации платежной системы (далее – ЦУКС) – регистрационный центр.

1. Общие положения.

1.1. Настоящий Регламент устанавливает порядок взаимодействия между Банком и Клиентом при работе с криптографическими ключами, применяемыми при формировании и передаче отчетности по форме 0409701.

1.2. В ходе функционирования Клиента им должны храниться заверенные регистрационные карточки сертификата ключей СКАД «Сигнатура» Клиента.

1.3. Контакты ЦУКС, сертификаты СКАД «Сигнатура», необходимые для взаимодействия с платежной системой Банка России при формировании и передаче отчетности по форме 0409701, размещаются Банком на официальном сайте Банка России в информационно-телекоммуникационной сети "Интернет" (далее – официальный сайт Банка России) по адресу:

http://www.cbr.ru/development/mcirabis/Involve_EM/.

1.4. Информация обо всех изменениях в процессе работы и управления криптографическими ключами доводится до Клиента путем размещения информационного письма и необходимых материалов на официальном сайте Банка России по адресу:

http://www.cbr.ru/development/mcirabis/acyoc/.

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;
- участие в рассмотрении спорных ситуаций между Клиентом и Банком по поводу подлинности ЭС.

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. Порядок регистрации и сертификации криптографических ключей Клиента

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

Тестовые криптографические ключи предназначены для организации взаимодействия с ССТ.

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.

3.1.4. При необходимости изготовления или плановой смены действующих тестовых ключей, Клиент направляет в ЦУКС по электронной почте на адрес, указанный на официальном ресурсе Банка 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 промышленных криптографических ключей Клиента в ЦУКС.

3.2.1. Клиент проходит процедуру регистрации криптографических ключей Клиента:

- при подключении к обмену электронными сообщениями;
- при смене наименования и/или организационно-правовой формы;
- при необходимости изготовления дополнительных криптографических ключей;
- при неисправности ключевого носителя или истечении срока действия криптографического ключа.

Процедура регистрации происходит в здании Банка по адресу, указанному на официальном сайте Банка России (п. 1.3).

3.2.2. Порядок получения криптографических ключей и сертификатов регистрации Клиента.

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

1 Заявление (Приложение 1) на получение администратором ключевой системы Клиента ключей и сертификатов регистрации (далее – Заявление);

- транспортный отчуждаемый машинный носитель информации (далее - ОМНИ) (рекомендуется flash-drive) для записи ключей и сертификатов регистрации;

- документ об уполномоченных лицах с образцами их подписи и оттиском печати Клиента (при ее наличии), заверенный руководителем Клиента (Приложение 2).

Примечание:

- ОМНИ должен быть отформатирован Клиентом и не должен содержать посторонней информации;
- при формировании ключа регистрации поле сертификата ключа «Наименование организации» заполняется АКС ЦУКС в точном соответствии с наименованием (полным или сокращенным), указанным в Заявлении.

В Заявлении Клиентом указывается необходимый тип криптографических ключей и их количество. Для обеспечения непрерывной и безотказной работы рекомендуется изготавливать не менее двух криптографических ключей 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)

3.2.2.2. Не позднее трех рабочих дней после подачи Заявления, АКС Клиента необходимо обратиться в ЦУКС по телефону, указанному на официальном сайте Банка России (п. 1.3.) для получения сведений о готовности ключевой информации.

3.2.2.3. За готовой ключевой информацией прибывает АКС Клиента. При себе необходимо иметь паспорт.

Выдача ключевой информации АКС осуществляется ежедневно в рабочие дни, адрес и время выдачи указаны на официальном сайте Банка России.

3.2.2.4. АКС Клиента получает:

- один экземпляр заверенной ЦУКС регистрационной карточки сертификата ключа регистрации на каждый ключ регистрации Клиента;
- сертификат регистрации и ключ регистрации на предоставленных ранее в качестве приложения к Заявлению ОМНИ (п. 3.2.2.1.).

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

Ключ регистрации действителен один календарный месяц со дня его формирования. В течение этого месяца процедура регистрации

криптографических ключей Клиента должна быть завершена.

3.2.2.5. АКС Клиента проверяет корректность заполнения полей сертификата: соответствие регистрационных данных, БИК, УИС, наименования организации, указанным в Заявлении, а также количество и тип изготовленных ключей.

При выявлении несоответствий в регистрационных данных, ключи регистрации не выдаются. Если ошибка была допущена при выработке ключа, АКС ЦУКС вырабатывает новый ключ.

Если ошибка была допущена в Заявлении, АКС Клиента направляет новое Заявление, АКС ЦУКС вырабатывает новый ключ.

3.2.2.6. Факт передачи ключа регистрации и факт проверки правильности заполнения полей сертификата организации, подтверждаются проставлением даты получения, подписей АКС Клиента (и АКС ЦУКС на каждой регистрационной карточке сертификата ключа регистрации Клиента. Один экземпляр регистрационной карточки сертификата ключа регистрации хранится в ЦУКС, второй экземпляр передается Клиенту.

3.3. Порядок сертификации криптографических ключей Клиента

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

Для отправки запросов необходимо:

1) архивировать запросы на получение сертификата (файлы **.pse)* в один файл (без создания папок) с именем:

Q_<краткое наименование организации>.zip (.rar)

(без создания папок);

2) направить сформированный файл в ЦУКС по электронной почте на адрес, указанный на официальном сайте Банка России (п. 1.3.), обязательно указав в теме письма:

701_ *<краткое наименование организации>;*

3) уведомить АКС ЦУКС по телефону, указанному на официальном сайте Банка России (п. 1.4.), 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 криптографических ключей, на действующем криптографическом ключе Клиента.

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

3.3.2. После получения запроса на получение сертификата АКС ЦУКС проводит сертификационные работы и готовит регистрационные карточки для передачи Клиенту, заверяет подписями АКС ЦУКС и печатью ЦУКС.

3.3.3. Уполномоченный представитель Клиента получает в Банке по два экземпляра регистрационной карточки на каждый криптографический ключ.

3.3.4. Уполномоченный представитель Клиента (доставляет в Банк по два экземпляра регистрационной карточки на каждый криптографический ключ, заверенные со стороны Клиента.

Примечание:

- при плановой смене ключа необходимо дополнительно предоставить документ (или его копию) об уполномоченных лицах с образцами их подписи и оттиском печати Клиента (при ее наличии), заверенный руководителем Клиента (п. 3.2.2.1.).

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

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

В случае отсутствия у Клиента возможности получения файла обновлений по электронной почте, АКС ЦУКС передает представителю Клиента сформированные сертификаты ключей на ОМНИ, предоставленном Клиентом, при личной явке в указанное выше время (п. 1.3.).

Примечание:

- получение Клиентом сертификатов ключей в электронном виде возможно только после предоставления в ЦУКС оформленных регистрационных карточек сертификатов ключей;

- сертификаты СКАД «Сигнатура» действующих криптографических ключей Банка, используемых для приема/передачи отчетности по форме 0409701, размещены на официальном сайте Банка России.

4. Порядок смены криптографических 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 криптографического ключа: Клиент (не менее, чем за три месяца до срока окончания действия криптографического ключа, должен организовать его плановую смену: формирование нового криптографического ключа и отправку запроса на получение сертификата в ЦУКС.

Порядок действий при сертификации новых ключей изложен в п. 3.3. настоящего Регламента.

4.3. Смена криптографических ключей Банка: Банк не позднее, чем за десять рабочих дней должен оповестить Клиента в установленном порядке о сроке предстоящей плановой смены криптографических ключей ключевых систем СКАД «Сигнатура» и о публикации необходимых обновлений (п. 1.4.).

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

4.5. Клиент берет на себя полную ответственность и обязуется обеспечивать сохранность, неразглашение сведений о криптографических ключах и нераспространение криптографических ключей неуполномоченным лицам. В случае, если Клиент разрешает третьим лицам использовать свои криптографические ключи, он несет полную ответственность за соблюдение условий Договора, как со своей стороны, так и со стороны, третьих лиц, пользующихся его криптографическими ключами.

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

Клиентом или Банком может быть принято решение о компрометации или досрочном прекращении срока действия криптографического ключа.

К компрометации ключа могут быть отнесены следующие события:

- утрата ключевого носителя;
- утрата ключевого носителя с последующим обнаружением;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нерасшифрование входящих или исходящих сообщений у Клиента;
- нарушение печати на сейфе с ключевыми носителями.

Первые три события должны трактоваться как безусловная компрометация действующих ключей, следующие события требуют специального рассмотрения в каждом конкретном случае.

Решение о компрометации ключа при увольнении или прекращении полномочий работника, имевшего доступ к криптографическому ключу, принимается Клиентом.

5.1. В случае принятия решения о компрометации криптографического

ключа, использование скомпрометированного криптографического ключа должно быть прекращено.

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

организует формирование запроса на отзыв сертификата;

по электронной почте (или на съемном носителе) передает запрос в ЦУКС;

сообщает в ЦУКС по телефону, указанному на официальном сайте Банка России о компрометации/досрочном прекращении срока действия криптографического ключа и отправке запроса на отзыв сертификата.

При отправке запроса по электронной почте необходимо:

- архивировать запрос на отзыв сертификата в файл с именем

Q_<*краткое наименование организации*>_отзыв.zip. (rar)

(без создания папок)

- направить сформированный файл в ЦУКС по электронной почте на адрес, указанный на официальном сайте Банка России, 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 или досрочном прекращении срока действия криптографических ключей» (далее – Уведомление).

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

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

САС 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 сайте Банка России, САС может быть выслан Клиенту на адрес отправителя запроса или передан уполномоченному 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 п. 3.2.2. настоящего Регламента.

5.5. При компрометации криптографического ключа Банка АКС ЦУКС формирует новый САС и направляет Клиенту информационное письмо и файл обновлений (п. 1.4.).

При получении информационного письма и файла обновлений от Банка, Клиент должен обработать файл обновлений на АРМ Клиента.