ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

УТВЕРЖДАЮ

Заместитель директора Департамента безопасности Банка России – директор Межрегионального центра безопасности Банка России

Ю.Г. Бочаров

Регламент взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платформы Цифрового рубля

(вторая редакция)

СОГЛАСОВАНО

Начальник Главного центра криптографической защиты информации (на правах Управления) Департамента безопасности Банка России

А.В. Быков

2023

Содержание

Обозначения и сокращения

АКС	Администратор ключевой системы
КК	Контур контроля
КО	Контур обработки
ЛК	Личный кабинет участника обмена
ПлЦР	Платформа Цифрового рубля Банка России
ПУЦ	Подчиненный удостоверяющий центр
РОРД	Регистрационный, операционный и расчетный депозитарий
САС	Список аннулированных сертификатов
СКЗИ	Средство криптографической защиты информации
ТШ КБР	Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России
УКЭП	Усиленная квалифицированная электронная подпись
УЦ ПлЦР	Подсистема «Удостоверяющий Центр Платформы Цифрового рубля Банка России»
ФП	Финансовый посредник
ЭС	Электронное сообщение

Термины «ключ электронной подписи», «ключ проверки электронной подписи», «сертификат ключа проверки электронной подписи» используются в значениях, определенных Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ.

В контексте данного Руководства под терминами «ключ» и «сертификат» подразумеваются «ключ электронной подписи» и «сертификат ключа проверки электронной подписи» соответственно.

Данный документ определяет порядок взаимодействия ФП с Банком России в части управления криптографическими ключами ПлЦР и является методическим руководством АКС ФП ПлЦР.

1.Общие положения

1.1. Взаимодействие с Банком России по вопросам управления ключами со стороны ФП осуществляется лицами, назначенными ФП ответственными за управление криптографическими ключами - АКС ФП, путем выдачи доверенности на право осуществлять функции АКС ФП. ФП должен организовать постоянное нахождение на рабочем месте в течение рабочего времени минимум одного АКС ФП. Форма доверенности определена в приложении к настоящему Регламенту.

1.2. ФП заблаговременно до окончания срока (либо при изменении каких-либо данных) доверенности направляет в Банк России обновленный экземпляр доверенности.

1.3. Управление криптографическими ключами осуществляется лицами, назначенными Банком России АКС ПлЦР (далее – АКС Банка). Взаимодействие с АКС Банка осуществляется с помощью электронной почты (cbdc-key@cbr.ru) или при личной явке АКС ФП к АКС Банка.

1.4. ФП для подключения к ПлЦР должен создать или переподчинить существующий Удостоверяющий Центр подсистеме Удостоверяющего Центра Платформы Цифрового рубля Банка России.

1.5. В рамках взаимодействия Банк России изготавливает следующие сертификаты ключей ФП:

- сертификат ПУЦ ФП;

- сертификаты КК ФП и КО ФП.

1.6. Для обеспечения безостановочного функционирования ПлЦР ФП изготавливает основные и резервные ключи КК ФП и КО ФП. Основные ключи КК ФП и КО ФП используются ФП для работы в ПлЦР. Резервные ключи КК ФП и КО ФП для работы в ПлЦР не используются. Резервные

ключи вводятся в действие в случае компрометации основных ключей КО ФП и КК ФП.

1.7. С каждого оригинала ключа (ключа ПУЦ ФП, основных и резервных ключей КК ФП и КО ФП) с помощью СКЗИ ФП изготавливает минимум по одной рабочей копии. Рабочие копии ключей используются для работы с ПлЦР. Оригиналы ключей используются только для изготовления рабочих копий ключей.

1.8. АКС ФП должен в установленные сроки выполнять все предписания, направленные АКС Банка.

1.9. ФП изготавливает криптографические ключи самостоятельно с использованием применяемого СКЗИ.

1.10. Эксплуатация СКЗИ должна производится в соответствии с требованиями эксплуатационной документации на применяемое СКЗИ.

1.11. ФП может начать использование ключей только после проведения процедуры их регистрации и сертификации в Банке России. Использование ключей после вывода их из действия (в том числе по причине компрометации) не допускается.

1.12. Банк России и ФП признают действительность сертификатов ключей ФП, исходя из того, что:

- указанные сертификаты подписаны ключом УЦ ПлЦР, переданного ответственному представителю ФП лично при проведении регистрации в Банке России, переданного через ЛК, либо полученного от Банка России иным способом, определяемым Банком России;

- регистрационные карточки указанных сертификатов изготовлены и оформлены ФП надлежащим образом в соответствии с разделом 13 настоящего Регламента и переданы в Банк России.

1.13. При необходимости Банк России предоставляет ФП копии регистрационных карточек сертификатов УЦ ПлЦР, КК, Узлов РОРД, Сервиса эмиссионных операций ПлЦР.

1.14. Банк России признает действительность запросов на сертификаты ключей, изготовленных ФП, в случае совпадения открытых ключей в запросах на сертификаты с открытыми ключами в оформленных регистрационных карточках запросов на сертификаты ФП, заверенных собственноручной подписью руководителя или АКС ФП, заверенную оттиском печати владельца ключа.

1.15. Для взаимодействия ФП с ПлЦР на тестовом стенде ПлЦР и в промышленной среде изготавливаются два отдельных комплекта ключей в двух отдельных ключевых системах.

1.16. Порядок изготовления ключевой информации для ТШ КБР определен в Регламенте взаимодействия Банка России и Клиента (косвенного участника Клиента), Пользователя при управлении криптографическими ключами.

1.17. ФП и Банк России при изготовлении сертификатов руководствуются документом «Платформа Цифрового рубля. Правила заполнения сертификатов».

1.18. При использовании системы криптографической защиты информации «Янтарь» изготовление ключей и сертификатов, необходимых для администрирования криптосерверов системы криптографической защиты информации «Янтарь» ФП, а также управление ими, осуществляется самостоятельно ФП в специально для этого предназначенной ключевой системе, отличной от ключевой системы ПлЦР.

1.19. Выдача сертификатов ФП проводится при условии идентификации ФП.

Идентификация проводится одним из следующих способов:

- при личном присутствии – путем прибытия АКС ФП в Банк России с документом, удостоверяющим личность.

- без личного присутствия, путем направления ФП запроса на выпуск сертификата через ЛК, подписанного усиленной квалифицированной электронной подписью ФП. При проведении идентификации заявителя без

его личного присутствия файлы запросов на выпуск сертификатов должны быть помещены в архив, архив подписан УКЭП ФП и направлен в Банк России через ЛК.

1.20. Взаимодействие АКС ФП с АКС Банка по электронной почте должно осуществляться с адресов, указанных в доверенности на право осуществлять функции АКС ФП (без использования функционала отправки письма от имени другого пользователя).

2. Основные функции Банка России и финансового посредника

2.1. Основными функциями Банка являются следующие:

- регистрация и сертификация ключей ФП;

- консультирование по вопросам регистрации и сертификации ключей;

- организация работ по плановой (или внеплановой) смене ключей ПлЦР, ФП;

- участие в рассмотрении спорных ситуаций между ФП и ПлЦР по поводу подлинности ЭС.

2.2. Основными функциями ФП являются следующие:

- обеспечение сохранности, неразглашение сведений о ключах и нераспространение ключей неуполномоченным лицам.

- регистрация и сертификация ключей пользователей ПлЦР;

- выполнение плановой (внеплановой) смены ключей ФП;

- выполнение работ, предписанных АКС Банка, в указанные сроки;

- комиссионное уничтожение выведенных из действия ключей ФП с составлением акта;

- доведение корневого сертификата УЦ ПлЦР и его САС до пользователей ПлЦР.

3. Порядок первичного изготовления ключей ФП

3.1. ФП до начала формирования ключей оформляет и представляет в Банк России на бумажном носителе доверенность на право осуществлять функции АКС ФП (указываются фамилия, инициалы, образец подписи, контактный номер телефона АКС ФП, e-mail для взаимодействия с АКС ФП по управлению ключами). В случае изменения сведений о АКС ФП, ФП обязан представить в Банк России актуальную информацию.

3.2. АКС Банка направляет на e-mail АКС ФП xml-файлы с информацией, необходимой для изготовления ключей КК и КО, ключа ПУЦ ФП и указание о порядке их обработки.

3.3. АКС ФП сверяет значения идентификатора участника и идентификатор кошелька участника, указанные в xml-файлах (поля «O» и «OU» соответственно) со значениями, полученными от Банка России. Остальные значения xml-файла сверяются в соответствии с документом «Платформа Цифрового рубля. Правила заполнения сертификатов».

В случае несовпадения полей в xml-файле АКС ФП сообщает об этом АКС Банка. До устранения несоответствий работы не проводятся.

3.4. ФП, используя полученные xml-файлы, генерирует основной и резервные ключи КК ФП и КО ФП, распечатывает на бумажном носителе запросы на сертификаты ключей (при возможности), сохраняет файлы запросов на сертификаты.

3.5. ФП, используя полученный xml-файл, генерирует ключ ПУЦ ФП, распечатывает на бумажном носителе запрос на сертификат ключа (при возможности), сохраняет файл запроса на сертификат ключа.

3.6. В случае совпадения идентификаторов, корректности полей и выбора прохождения идентификации ФП путем личного присутствия АКС ФП направляет на e-mail АКС Банка файлы с запросами на сертификаты основного и резервного ключей КК и КО, ключа ПУЦ ФП.

В случае совпадения идентификаторов, корректности полей и выбора прохождения идентификации ФП без личного присутствия АКС ФП

направляет через ЛК архив с файлами запросов на сертификаты основного и резервного ключей КК и КО, ключа ПУЦ ФП, подписанный УКЭП ФП.

3.7. АКС ФП оформляет в одном экземпляре регистрационные карточки запроса на сертификаты основного и резервных ключей КК ФП и КО ФП, ключа ПУЦ ФП в соответствии с требованием раздела 13 настоящего Регламента. Оформленные регистрационные карточки запроса на сертификаты направляются ФП в Банк России способом, обеспечивающим их быструю и надежную передачу.

3.8. ФП с помощью СКЗИ изготавливает с оригиналов ключей рабочие копии. Для работы в рамках ПлЦР используются рабочие копии основного ключа КК и КО, ключа ПУЦ ФП.

3.9. Банк России получает заверенные регистрационные карточки запросов на сертификаты ключей ФП и файлы запросов на сертификаты, производит их проверку.

3.10. В случае нахождения несоответствия в полученных от ФП файлах с запросами на сертификаты, или ошибки в оформлении регистрационных карточек запросов на сертификаты, на e-mail АКС ФП направляется соответствующее сообщение. До устранения замечаний регистрация и сертификация ключей не производится.

3.11. АКС Банка направляет на e-mail АКС ФП сообщение об успешной проверке регистрационных карточек запросов на сертификаты.

3.11.1. В случае проведения идентификации путем личного присутствия согласовывает время прибытия АКС ФП в Банк России для проведения дальнейших работ по регистрации сертификатов ключей ФП в УЦ ПлЦР Банка России и идентификации ФП.

АКС ФП прибывает в Банк России с документом, удостоверяющим личность. АКС Банка проверяет права АКС ФП в соответствии с доверенностью и, в случае успешной проверки, производит передачу АКС ФП следующих файлов:

- сертификаты основных и резервных ключей КК и КО;

- сертификат ключа ПУЦ ФП;

- сертификат УЦ ПлЦР Банка России;

- САС УЦ ПлЦР Банка России.

Передача файлов оформляется актом в произвольной форме.

3.11.2. В случае прохождения идентификации без личного присутствия файлы, указанные в пункте 3.11.1, направляются в адрес ФП через ЛК с дополнительным оповещением АКС ФП через e-mail.

3.12. АКС ФП осуществляет обработку поступивших от АКС Банка файлов.

ФП выпускает САС ПУЦ ФП в соответствии с требованиями раздела 4 настоящего Регламента. Выгружает САС ПУЦ ФП в DER кодировке. АКС ФП направляет файл с САС ПУЦ ФП в DER кодировке в адрес АКС Банка по e-mail.

3.13. АКС Банка направляет письмо на e-mail АКС ФП с информацией о результате загрузки САС ПУЦ ФП в УЦ ПлЦР.

3.14. АКС ФП, распечатывает в двух экземплярах регистрационные карточки сертификатов ключей КК ФП и КО ФП, ключа ПУЦ ФП, оформляет их в соответствии с требованием раздела 13 настоящего Регламента. Первые экземпляры на бумажном носителе заверенных регистрационных карточек сертификатов остаются у ФП, вторые экземпляры на бумажном носителе направляются ФП в Банк России способом, обеспечивающим их быструю и надежную передачу.

3.15. Банк России получает заверенные регистрационные карточки сертификатов ключей ФП и производит их проверку. В случае нахождения ошибок в оформлении регистрационных карточек сертификатов на e-mail АКС ФП направляется соответствующее сообщение. До устранения замечаний дальнейшие работы не производятся.

3.16. АКС Банка направляет на e-mail АКС ФП сообщение об успешной регистрации ключей, а также сертификаты КК, Узлов РОРД и Сервиса Эмиссионных операций ПлЦР.

3.17. АКС ФП обрабатывает, полученные в пункте 3.16 сертификаты.

4. Сроки действия и порядок выпуска списка аннулированных сертификатов

4.1. Срок действия САС ПУЦ ФП – 35 дней.

4.2. ФП производит выпуск САС ПУЦ ФП не реже одного раза в 7 дней и в случае аннулирования сертификата пользователя ПлЦР.

4.3. ФП при выпуске нового САС направляет его на ПлЦР с использованием альбома ЭС.

При отсутствии подтверждения об успешной загрузке САС в ПлЦР АКС ФП обращается в Банк России установленным порядком.

4.4. Банк России направляет САС УЦ ПлЦР в адрес ФП, используя ЛК, либо иным способом, определенным Банком России, с дополнительным оповещением АКС ФП по e-mail.

4.4. АКС ФП осуществляет обработку поступившего от Банка России САС УЦ ПлЦР.

4.5. АКС ФП организует передачу САС УЦ ПлЦР пользователям ПлЦР в сроки, определенные АКС Банка.

5. Плановая смена ключей КК ФП и КО ФП

5.1. АКС ФП за 2 месяца до окончания срока действия ключей КК и КО ФП обращается к АКС Банка. АКС Банка направляет на e-mail АКС ФП xml-файлы с информацией, необходимой для изготовления ключей КК и КО, указание о порядке их обработки

ФП производит генерацию основных и резервных ключей «новой» серии КК ФП и КО ФП, распечатывает запросы на сертификаты ключей «новой» серии (при возможности), сохраняет файлы запросов на сертификат ключей.

В случае выбора прохождения идентификации ФП путем личного присутствия направляет на e-mail АКС Банка файлы с запросами на сертификаты основного и резервного ключей КК и КО.

В случае выбора прохождения идентификации ФП без личного присутствия направляет через ЛК архив с файлами запросов на сертификаты основного и резервного ключей КК ФП и КО ФП, подписанный УКЭП ФП.

5.2. АКС ФП оформляет в одном экземпляре регистрационные карточки запроса на сертификаты основного и резервного ключей КК ФП и КО ФП в соответствии с требованием раздела 13 настоящего Регламента. Оформленные регистрационные карточки запроса на сертификаты направляются ФП в Банк России способом, обеспечивающим их быструю и надежную передачу.

5.3. Банк России получает заверенные регистрационные карточки запросов на сертификаты ключей ФП и файлы запросов на сертификаты, производит их проверку.

5.4. В случае нахождения несоответствия в полученных от ФП файлах с запросами на сертификаты, или ошибки в оформлении регистрационных карточек запросов на сертификаты, на e-mail АКС ФП направляется соответствующее сообщение. До устранения замечаний регистрация и сертификация ключей не производится.

5.5. АКС Банка направляет на e-mail АКС ФП сообщение об успешной проверке регистрационных карточек запросов на сертификаты.

5.5.1. В случае проведения идентификации путем личного присутствия согласовывает время прибытия АКС ФП в Банк России для проведения дальнейших работ по плановой смене ключей КК ФП, КО ФП.

АКС ФП прибывает к АКС Банка с документом, удостоверяющим личность. АКС Банка проверяет права АКС ФП в соответствии с доверенностью и, в случае успешной проверки, производит передачу АКС ФП сертификатов основных и резервных ключей КК ФП и КО ФП «новой серии».

Передача сертификатов оформляется актом в произвольной форме.

5.5.2. В случае прохождения идентификации без личного присутствия файлы, указанные в пункте 5.5.1, направляются в адрес ФП через ЛК с дополнительным оповещением АКС ФП через e-mail.

5.6. АКС ФП осуществляет обработку поступивших от АКС Банка файлов.

5.7. ФП распечатывает регистрационные карточки сертификатов основного и резервного ключей «новой» серии (серию ключа можно определить по полю «Описание» сертификата), оформляет их в соответствии с требованием раздела 13 настоящего Регламента. Первые экземпляры заверенных регистрационных карточек сертификатов остаются у ФП, вторые экземпляры на бумажном носителе направляются ФП в Банк России способом, обеспечивающим быструю и надежную передачу.

5.8. Банк России получает заверенные регистрационные карточки сертификатов ключей ФП и производит их проверку. В случае нахождения ошибок в оформлении регистрационных карточек сертификатов на e-mail АКС ФП направляется соответствующее сообщение. До устранения замечаний дальнейшие работы не производятся.

5.9. АКС Банка направляет на e-mail АКС ФП сообщение об успешной проверке регистрационных карточек сертификатов и вводе в действие ключей КК ФП и КО ФП «новой» серии.

5.10. ФП проводит работы по вводу в эксплуатацию ключей КК ФП и КО ФП «новой» серии. Работы по изготовлению ключей завершены. С этого момента для работы с ПлЦР используются основные ключи КК ФП и КО ФП «новой» серии.

5.11. В течение 10 дней после перехода на ключи «новой» серии АКС ФП необходимо провести уничтожение ключей ФП «старой серии». Уничтожение проводится в соответствии с разделом 12 настоящего Регламента.

6. Плановая смена ключей ПУЦ ФП

6.1. АКС ФП за 2 месяца до окончания срока действия ключа ПУЦ ФП обращается к АКС Банка. АКС Банка направляет на e-mail АКС ФП xml-файл с информацией, необходимой для изготовления ключа ПУЦ ФП и указание о порядке его обработки.

ФП выполняет генерацию ключа «новой» серии ПУЦ ФП и запроса на сертификат (при возможности).

В случае выбора прохождения идентификации ФП путем личного присутствия направляет на e-mail АКС Банка файл с запросом на сертификат ПУЦ ФП.

В случае выбора прохождения идентификации ФП без личного присутствия направляет через ЛК архив с файлом запроса на сертификат ПУЦ ФП, подписанный УКЭП ФП.

6.2. АКС ФП распечатывает в одном экземпляре регистрационную карточку запроса на сертификат ключа ПУЦ ФП, оформляет ее в соответствии с требованием раздела 13 настоящего Регламента. Оформленная регистрационная карточка запроса на сертификат направляется ФП в Банк России способом, обеспечивающим ее быструю и надежную передачу.

6.3. Банк России получает заверенную регистрационную карточку запроса на сертификат ключа ПУЦ ФП и файл запроса на сертификат, производит их проверку.

6.4. В случае нахождения несоответствия в полученных от ФП файлах с запросами на сертификаты, или ошибки в оформлении регистрационной карточке запроса на сертификат, на e-mail АКС ФП направляется соответствующее сообщение. До устранения замечаний регистрация и сертификация ключей не производится.

6.5. АКС Банка направляет на e-mail АКС ФП сообщение об успешной проверке регистрационной карточки запроса на сертификат.

6.5.1. В случае проведения идентификации путем личного присутствия согласовывает время прибытия АКС ФП в Банк России для проведения дальнейших работ по плановой смене ключа ПУЦ ФП.

АКС ФП прибывает к АКС Банка с документом, удостоверяющим личность. АКС Банка проверяет права АКС ФП в соответствии с доверенностью и, в случае успешной проверки, производит передачу АКС ФП сертификата ПУЦ ФП «новой серии».

Передача сертификата оформляется актом в произвольной форме.

6.5.2. В случае прохождения идентификации без личного присутствия сертификат ПУЦ ФП направляется в адрес ФП через ЛК с дополнительным оповещением АКС ФП через e-mail.

6.6. ФП осуществляет обработку поступившего от АКС Банка файла.

ФП делает загруженный сертификат «новой» серии ПУЦ ФП рабочим, выпускает САС ПУЦ ФП в соответствии с требованиями раздела 4 настоящего Регламента. Выгружает САС ПУЦ ФП в DER кодировке. АКС ФП направляет файл с САС ПУЦ ФП в DER кодировке в адрес АКС Банка по e-mail. Возвращает сертификат «текущей» серии ПУЦ ФП в статус «рабочий».

6.7. АКС Банка направляет письмо на e-mail АКС ФП с информацией о результате загрузки САС ПУЦ ФП в УЦ ПлЦР.

6.8. АКС ФП распечатывает регистрационную карточку сертификата ключа ПУЦ ФП «новой» серии, оформляет их в соответствии с требованием раздела 13 настоящего Регламента. Первый экземпляр заверенной регистрационной карточки сертификата остается у ФП, второй экземпляр направляется ФП в Банк России способом, обеспечивающим быструю и надежную передачу.

6.9. Банк получает заверенную регистрационную карточку сертификата ключа ПУЦ ФП и производит ее проверку. В случае нахождения ошибок в оформлении регистрационной карточки сертификата

на e-mail АКС ФП направляется соответствующее сообщение. До устранения замечаний дальнейшие работы не производятся.

6.10. АКС Банка направляет на e-mail АКС ФП сообщение об успешной проверке регистрационной карточки сертификата и вводе в действие ключа ПУЦ ФП «новой» серии.

6.11. АКС ФП организует доведение сертификата ПУЦ ФП до клиентов, при необходимости.

6.12. С этого момента для работы с ПУЦ ФП может использоваться ключ «новой» серии.

6.13. В течение 10 дней после перехода на ключ «новой» серии АКС ФП необходимо провести уничтожение ключа ПУЦ ФП «старой серии». Уничтожение проводится в соответствии с разделом 12 настоящего Регламента.

7. Плановая смена ключей УЦ ПлЦР Банка России

7.1. АКС Банка направляет АКС ФП сообщение о проведении работ по плановой смене ключей УЦ ПлЦР. В сообщении указывается номер новой серии ключей (например, Серия 2).

7.2. Банк России направляет сертификат УЦ ПлЦР «новой» серии и его САС в адрес ФП, используя ЛК, либо иным способом, определенным Банком России.

7.3. АКС ФП осуществляет обработку поступивших от Банка России файлов.

7.4. АКС ФП организует передачу сертификата УЦ ПлЦР «новой» серии и его САС клиентам в сроки, определенные АКС Банка.

7.5. ФП направляет письмо в Банк России с информацией о завершении работ, предписанных пунктом 7.4 настоящего Регламента.

8. Плановая смена ключа КК/Узлов РОРД/Сервиса Эмиссионных операций ПлЦР и других технологических ключей (при наличии)

8.1. АКС Банка направляет АКС ФП по электронной почте сертификаты КК/Узлов РОРД/Сервиса Эмиссионных операций ПлЦР и других технологических ключей (при наличии).

8.2. ФП осуществляет обработку сертификатов, поступивших от АКС Банка в пункте 8.1.

9. Хранение сертификатов ключевой системы ПлЦР Банка России

ФП обеспечивает архивное хранение сертификатов УЦ ПлЦР Банка России, сертификатов КК ФП и КО ФП, сертификатов ПУЦ ФП в течение срока их действия.

10. Порядок внеплановой смены основного ключа КК ФП и КО ФП

10.1. Внеплановая смена основного ключа КК или КО ФП проводится по инициативе ФП.

10.2. ФП проводит следующие действия по переходу на работу с резервным ключом:

- загружает справочник сертификатов с помощью основного ключа;
- подготавливает запрос на отзыв сертификата основного ключа и сохраняет его в файл;
- устанавливает в качестве рабочего сертификат резервного ключа;
- завершает работу со справочником сертификатов. С этого момента для работы с КК/КО используется резервный ключ, который переходит в статус основного.

10.3. АКС ФП направляет на e-mail АКС Банка уведомление о переходе на резервный ключ и файл с запросом на отзыв основного ключа для проведения АКС Банка мероприятий по отзыву сертификата основного ключа.

10.4. В течение 10 дней после перехода на работу с резервным ключом АКС ФП необходимо провести уничтожение выведенного основного ключа. Уничтожение проводится в соответствии с разделом 12 настоящего Регламента.

10.5. АКС Банка проводит мероприятия по отзыву сертификата основного ключа и направляет АКС ФП CAC, в котором аннулирован основной сертификат КК/КО.

10.6. ФП обрабатывает полученный файл с CAC, проверяет, что сертификат основного ключа аннулирован.

10.7. Далее необходимо провести работы по изготовлению нового резервного ключа КК/КО. Работы проводятся по аналогии с работами, описанными в разделе 3 Регламента в части ключей КК ФП и КО ФП.

11. Порядок действий в случае компрометации ключей ФП

11.1. Компрометацией ключей называется событие, приводящее к утрате доверия к тому, что используемые ключи обеспечивают безопасность информации. К основным событиям, приводящим к компрометации ключей, относятся, включая, но не ограничиваясь, следующие события:

− утрата ключевых носителей;

− утрата ключевых носителей с последующим обнаружением;

− увольнение сотрудников, имевших доступ к ключевой информации;

− нарушение правил хранения и уничтожения (после окончания срока действия) ключей ЭП;

− возникновение подозрений на нарушение конфиденциальности, целостности и доступности информации, передаваемой с использованием ключевой информации;

− нарушение печати на сейфе, в котором хранятся ключевые носители;

− случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что выход из строя произошел в результате несанкционированных действий злоумышленника).

Также к событиям компрометации относятся события, описанные в документации на применяемое СКЗИ.

11.2. В случае подозрения на компрометацию основного ключа КК/КО, АКС ФП выполняет работы по переходу на использование резервного ключа. На e-mail АКС Банка направляется уведомление о компрометации основного ключа. Работы по внеплановой смене основного ключа ФП производятся в соответствии с разделом 10 настоящего Регламента.

11.3. В случае подозрения на компрометацию резервного ключа КК/КО проводятся работы, описанные в разделе 10 настоящего Регламента с учетом того, что основной ключ КК/КО не скомпрометирован, а производится смена резервного ключа КК/КО.

11.4. В случае компрометации основного и резервного ключей КК/КО, АКС ФП незамедлительно сообщает об этом в Банк России, далее подготавливает уведомление о компрометации основного и резервного ключей КК/КО, подписанное руководителем ФП, и направляет его в Банк России способом, обеспечивающим его быструю и надежную передачу. Работа ФП с ПлЦР Банка России прекращается до изготовления и ввода в действие новых основного и резервных ключей КК/КО. Работы по изготовлению новых основного и резервного ключей производятся в соответствии с разделом 3 настоящего Регламента.

11.5. При компрометации ключа ПУЦ ФП скомпрометированными считаются все сертификаты, изготовленные с использованием данного ПУЦ ФП. Ключевая система разворачивается заново, начиная с получения xml-

файла для ПУЦ ФП и изготовлением новой ключевой информации всем пользователям.

11.6. При компрометации действующего ключа ПУЦ ФП АКС ФП должен незамедлительно сообщить об этом АКС Банка. ФП направляет в Банк России письмо за подписью руководителя с описанием ситуации. АКС Банка будут организованы работы по внеплановой смене ключа ПУЦ ФП.

12. Порядок уничтожения ключей

12.1. Выведенные из действия ключи (оригиналы и рабочие копии) уничтожаются ФП самостоятельно. Для уничтожения создается комиссия, состоящая не менее чем из трех человек. По результатам работы комиссии составляется акт. Информация о проведенных работах об уничтожении ключей должна быть доведена АКС ФП до Банка России (с указанием номера и даты акта) посредством сообщения на e-mail АКС Банка.

13. Порядок изготовления регистрационной карточки сертификата ключей ФП

13.1. Регистрационная карточка сертификата открытого ключа ФП формируется АКС ФП в справочнике сертификатов из сертификата открытого ключа ФП и должна содержать, в том числе:

- наименование организации владельца ключа сертификата;

- наименование применяемого СКЗИ;

- информацию, идентифицирующую ключ и соответствующий ему сертификат открытого ключа (идентификатор и (или) номер ключа, идентификатор и (или) номер серии);

- информацию о назначении ключа (область применения);

- серийный номер открытого ключа в шестнадцатеричной системе счисления;

- даты начала и окончания действия ключа и соответствующего ему сертификата открытого ключа;

- фамилию и инициалы, должность и собственноручную подпись руководителя или АКС ФП, заверенную оттиском печати владельца ключа.

Сертификат ключа ФП подписан ключом УЦ ПлЦР Банка России, переданного АКС ФП по доверенному каналу, что является фактом подтверждения изготовления сертификата Банком России.

Регистрационная карточка сертификата ключа может распечатываться на одном или нескольких листах. При распечатке регистрационной карточки на нескольких листах каждый лист должен содержать собственноручную подпись руководителя или АКС ФП, заверенную оттиском печати владельца ключа.

13.2. Регистрационная карточка сертификата каждого ключа изготавливается в двух экземплярах. Один экземпляр хранится в Банке России, другой – у ФП. Ключ считается зарегистрированным после передачи в Банк России надлежащим образом заверенного экземпляра оформленной регистрационной карточки сертификата ключа.

14. Порядок получения тестовой ключевой информации

14.1. Порядок получения тестовой ключевой информации для взаимодействия ФП с ПлЦР на тестовом стенде ПлЦР аналогичен порядку получения промышленной ключевой информации, с учетом того, что печать, оформление, направление в Банк России экземпляров регистрационных карточек запросов на сертификаты и сертификатов ключей ФП и идентификация ФП не производится. Информация об уничтожении ФП тестовых ключей до Банка России не доводится. Взаимодействие происходит между АКС Банка и АКС ФП происходит с использованием e-mail.

Приложение

Форма Доверенности АКС ФП

ДОВЕРЕННОСТЬ
на право осуществления функций администратора ключевой системы финансового посредника

Страна, город, число

Наименование организации, в лице *должность ФИО*, действующего на основании *Устава*, настоящей доверенностью уполномочивает *должность, ФИО*[1] *(номер телефона, эл. почта), должность, ФИО (номер телефона, эл. почта)* осуществлять функции ответственного за управление криптографическими ключами в рамках взаимодействия с Платформой Цифрового рубля.

Предоставленные полномочия могут осуществляться каждым из перечисленных сотрудников в отдельности.

Полномочия по настоящей доверенности не могут быть переданы другим лицам.

Подпись *ФИО* _____ удостоверяю
(подпись доверенного лица)
Подпись *ФИО* _____ удостоверяю
(подпись доверенного лица)

Настоящая доверенность выдана на срок по *дата*.

*Должность*_____ *ФИО*
(подпись)

[1] Количество лиц, ответственных за управление криптографическими ключами, должно быть не менее двух.