

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

УТВЕРЖДАЮ

Заместитель директора Департамента
безопасности Банка России

А.А. Каршин

**Регламент
взаимодействия Финансового посредника и Банка России
при управлении криптографическими ключами
Платформы Цифрового рубля
(третья редакция)**

СОГЛАСОВАНО

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

С.Н. Смирнов

Содержание

Обозначения и сокращения	3
1. Общие положения	4
2. Основные функции Банка России и финансового посредника при управлении криптографическими ключами ПлЦР.....	8
3. Порядок первичного изготовления ключей ФП.....	9
4. Сроки действия и порядок выпуска списка аннулированных сертификатов 11	
5. Периоды использования ключей ПУЦ ФП	12
6. Смена ключей КК ФП и КО ФП.....	12
7 Смена ключей ПУЦ ФП.....	14
8. Смена ключей УЦ ПлЦР Банка России	16
9. Смена ключей компонентов ПлЦР	17
10. Порядок действий в случае компрометации ключей ФП.....	17
11. Порядок уничтожения ключей.....	19
12. Порядок изготовления регистрационной карточки сертификата ФП.....	19
13. Порядок получения тестовой ключевой информации	20

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
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

1. Общие положения

1.1. Регламент взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платформы Цифрового рубля (далее – Регламент) определяет порядок взаимодействия ФП с Банком России в части управления криптографическими ключами ПлЦР и является методическим руководством АКС ФП.

1.2. 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.

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

1.4. Ключи (или сертификаты) «новой» серии – ключи (или сертификаты), планируемые к вводу в действие после успешного прохождения процедуры смены.

Ключи (или сертификаты) «текущей» серии – ключи (или сертификаты), введенные в действие и используемые в данный момент времени.

1.5. Регистрационная карточка сертификата – документ на бумажном носителе, содержащий информацию о сертификате.

1.6. 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;

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);

события, определенные в документации на применяемое СКЗИ, как компрометация.

1.7. Взаимодействие с Банком России по вопросам управления ключами со стороны ФП осуществляется лицами, ответственными за управление криптографическими ключами – АКС ФП, на основании выданной ФП доверенности на право осуществления функций АКС ФП участника платформы цифрового рубля (далее – доверенность). Форма доверенности определена в Стандарте платформы цифрового рубля «Порядок подключения участника платформы к платформе цифрового рубля».

1.8. ФП заблаговременно до окончания срока (либо при изменении каких-либо данных) доверенности направляет в подразделение Банка России, обслуживающее счет цифрового рубля ФП, обновленный экземпляр доверенности.

1.9. Управление криптографическими ключами на стороне Банка России осуществляется лицами, назначенными Банком России АКС УЦ ПлЦР (далее – АКС Банка). Взаимодействие АКС ФП с АКС Банка осуществляется посредством электронной почты (cbdc-key@cbr.ru).

1.10. В рамках взаимодействия Банк России изготавливает следующие сертификаты ФП:

- сертификат ПУЦ ФП;
- сертификаты КК ФП и КО ФП.

Порядок изготовления ключевой информации для ТШ КБР в настоящем Регламенте не рассматривается.

1.11. Для обеспечения непрерывного и безотказного взаимодействия с 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.

1.12. Объекты ключевой системы ПлЦР, подлежащие обмену между АКС ФП и АКС Банка, должны быть представлены в DER либо в PEM кодировке.

1.13. АКС ФП должен в установленные сроки выполнять все указания, направленные АКС Банка.

1.14. АКС ФП запрещается удалять сертификаты компонентов ПлЦР из справочников/хранилищ сертификатов ФП без предписания АКС Банка.

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

1.16. Эксплуатация СКЗИ должна производиться в соответствии с требованиями эксплуатационной документации на применяемое СКЗИ.

1.17. Запрещается организация функционирования на одном ключе и сертификате ПУЦ ФП двух и более независимых друг от друга удостоверяющих центров.

1.18. ФП может начать использование ключей только после проведения процедуры их ввода в действие в Банке России. Использование ключей после вывода их из действия (в том числе по причине компрометации) не допускается.

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

указанные сертификаты подписаны ключом УЦ ПлЦР, сертификат которого передан АКС ФП лично при проведении идентификации в Банке России либо получен ФП от Банка России иным способом, определяемым Банком России;

указанные сертификаты соответствуют требованиям документа «Платформа Цифрового рубля. Правила заполнения полей сертификатов»;

срок действия сертификатов не истек;

сертификаты не аннулированы;

регистрационные карточки указанных сертификатов оформлены ФП надлежащим образом в соответствии с разделом 12 настоящего Регламента и переданы в Банк России.

1.20. При необходимости Банк России предоставляет ФП копии регистрационных карточек сертификатов компонентов ПлЦР и УЦ ПлЦР.

1.21. Для взаимодействия ФП с ПлЦР в тестовой и в промышленной средах изготавливаются два отдельных комплекта ключей в соответствующих ключевых системах.

1.22. ФП при создании запросов на сертификаты руководствуются документом «Платформа Цифрового рубля. Правила заполнения полей сертификатов».

1.23. Выдача сертификатов ФП проводится при условии идентификации ФП. Идентификация проводится одним из следующих способов:

при личном присутствии;

без личного присутствия.

1.24. Взаимодействие АКС ФП с АКС Банка по электронной почте должно осуществляться с адресов, указанных в доверенности на право осуществлять функции АКС ФП (функционал отправки письма от имени другого пользователя допускается только от имени АКС ФП). ФП

обеспечивает возможность получения электронных писем от АКС Банка на данный адрес электронной почты.

1.25. ФП перед началом работ по первичному изготовлению ключей направляет в Департамент безопасности Банка России письмо с информацией о наличии/отсутствии технической возможности создания ключей промышленного ПУЦ ФП сроком действия 36 месяцев и их записи на используемые ФП ключевые носители.

ФП при изменении статуса технической возможности создания ключей промышленного ПУЦ ФП сроком действия 36 месяцев и их записи на используемые ФП ключевые носители направляет в Департамент безопасности Банка России соответствующее письмо.

2. Основные функции Банка России и финансового посредника при управлении криптографическими ключами ПлЦР

2.1. Основными функциями Банка России при управлении криптографическими ключами ПлЦР являются следующие:

создание и аннулирование сертификатов ФП;

консультирование по вопросам создания ключей и сертификатов ФП;

организация работ по смене ключей компонентов ПлЦР.

2.2. Основными функциями ФП при управлении криптографическими ключами ПлЦР являются следующие:

выполнение работ по созданию ключей ФП;

выполнение работ по смене ключей ФП;

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

создание и аннулирование сертификатов пользователей ПлЦР;

контроль за сроками действия ключей ФП;

выполнение в указанные сроки работ, предписанных АКС Банка;

уничтожение выведенных из действия ключей ФП;

обеспечение возможности аннулирования выпущенных сертификатов на протяжении срока действия их ключей.

3. Порядок первичного изготовления ключей ФП

3.1. ФП направляет в Департамент безопасности Банка России письмо с информацией о наличии/отсутствии технической возможности создания ключей промышленного ПУЦ ФП сроком действия 36 месяцев и их записи на используемые ФП ключевые носители.

3.2. ФП создает основные и резервные ключи КК ФП и КО ФП, сохраняет файлы запросов на сертификаты в формате PKCS#10.

ФП создает ключ ПУЦ ФП, сохраняет файл запроса на сертификат в формате PKCS#10.

При необходимости АКС ФП запрашивает у АКС Банка xml-файлы с информацией, необходимой для изготовления ключей КК ФП и КО ФП, ключа ПУЦ ФП. АКС Банка направляет запрошенную информацию в адрес АКС ФП по электронной почте.

3.3. АКС ФП сообщает АКС Банка по электронной почте выбранный способ идентификации ФП.

3.4. В случае прохождения идентификации ФП путем личного присутствия АКС ФП направляет одним сообщением на электронную почту АКС Банка файлы с запросами на сертификаты основного и резервного ключей КК и КО, ключа ПУЦ ФП. АКС Банка согласовывает с АКС ФП адрес и время прибытия АКС ФП в Банк России для проведения дальнейших работ по созданию сертификатов и идентификации ФП.

В случае прохождения идентификации ФП без личного присутствия АКС ФП направляет через ЛК в адрес Департамента безопасности Банка России архив с файлами запросов на сертификаты основного и резервного ключей КК и КО, ключа ПУЦ ФП, подписанный УКЭП ФП, с сопроводительным письмом. Допускается подписание архива с файлами запросов на сертификаты УКЭП ФП средствами ЛК.

3.5. В случае прохождения идентификации путем личного присутствия АКС ФП прибывает в Банк России с документом, удостоверяющим личность. АКС Банка/работник подразделения Банка России проверяет полномочия АКС ФП в соответствии с доверенностью и, в случае успешной проверки, производит передачу АКС ФП следующих файлов:

сертификаты основных и резервных ключей КК ФП и КО ФП;

сертификат ПУЦ ФП;

сертификат(ы) УЦ ПлЦР Банка России;

САС УЦ ПлЦР Банка России.

Передача файлов оформляется актом в произвольной форме.

3.6. В случае прохождения идентификации без личного присутствия файлы, указанные в пункте 3.5, направляются в адрес ФП через ЛК с дополнительным оповещением АКС ФП по электронной почте.

3.7. АКС Банка направляет в адрес ФП через ЛК файлы визуализации регистрационных карточек сертификатов ФП в формате «.pdf» с сопроводительным письмом. АКС ФП распечатывает в двух экземплярах файлы визуализации регистрационных карточек сертификатов КК ФП и КО ФП, ПУЦ ФП, оформляет их в соответствии с требованиями раздела 12 настоящего Регламента. Первые экземпляры на бумажном носителе заверенных регистрационных карточек сертификатов остаются у ФП, вторые экземпляры на бумажном носителе направляются ФП с сопроводительным письмом в подразделение Банка России, обслуживающее счет цифрового рубля ФП.

3.8. ФП выпускает САС ПУЦ ФП в соответствии с требованиями раздела 4 настоящего Регламента. АКС ФП направляет файл с САС ПУЦ ФП в адрес АКС Банка по электронной почте. Последующие САС направляются на ПлЦР в соответствии с требованиями раздела 4 настоящего Регламента.

3.9. АКС Банка направляет письмо на электронную почту АКС ФП с информацией о результате загрузки САС ПУЦ ФП в УЦ ПлЦР.

3.10. АКС Банка производит проверку регистрационных карточек сертификатов ФП. В случае нахождения ошибок в оформлении регистрационных карточек сертификатов на электронную почту АКС ФП направляется соответствующее сообщение. До устранения замечаний дальнейшие работы не проводятся.

3.11. В случае успешной проверки регистрационных карточек сертификатов ФП АКС Банка направляет на электронную почту АКС ФП сообщение об успешном завершении создания сертификатов ФП, а также сертификаты компонентов ПлЦР, необходимые для взаимодействия с ПлЦР

3.12. АКС ФП подтверждает получение сертификатов, направленных в соответствии с пунктом 3.11 настоящего Регламента.

4. Сроки действия и порядок выпуска списка аннулированных сертификатов

4.1. Банк России направляет САС УЦ ПлЦР в адрес ФП, используя ЛК, либо иным способом, определенным Банком России, с дополнительным оповещением АКС ФП по электронной почте.

4.2. Срок действия САС ПУЦ ФП – 35 дней.

4.3. ФП производит выпуск САС ПУЦ ФП не реже одного раза в 7 дней и в случае прекращения действия сертификата пользователя ПлЦР в соответствии с требованиями пункта 7 статьи 14 Федерального закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ.

4.4. ФП при выпуске САС (за исключением САС подготовленных в рамках первичного изготовления (п. 3.8) и смены (п. 7.9) ключей ПУЦ ФП) направляет его на ПлЦР с использованием Альбома ЭС.

4.5. ФП при приближении окончания срока действия ключа ПУЦ ФП выпускает САС с окончанием срока действия равному окончанию срока действия сертификата ПУЦ ФП (далее – финализированный САС).

4.6. АКС ФП направляет финализированный САС на ПлЦР с использованием Альбома ЭС и в адрес АКС Банка по электронной почте.

4.7. При необходимости аннулирования сертификата пользователя после выпуска финализированного САС, ФП осуществляет работы по аннулированию сертификата и повторяет действия, описанные в пунктах 4.5 и 4.6 настоящего Регламента.

5. Периоды использования ключей ПУЦ ФП

5.1. ФП определяет два периода использования ключа ПУЦ ФП. В первый период ключ ПУЦ ФП используется для подписания сертификатов и САС, во второй период – только для подписания САС.

5.2. Вне зависимости от срока действия криптографического ключа ПУЦ ФП, ФП должен обеспечить возможность аннулирования выпущенных сертификатов на протяжении срока действия их ключей.

6. Смена ключей КК ФП и КО ФП

6.1. Смену ключей КК ФП и КО ФП инициирует АКС ФП.

6.2. Смена ключей по причине окончания срока действия основных ключей должна быть инициирована АКС ФП не позднее чем за 2 месяца до окончания срока их действия и проведена одновременно для всех действующих ключей КК ФП и КО ФП (основных и резервных).

6.3. ФП создает основной и резервные ключи КК ФП и/или КО ФП, сохраняет файлы запросов на сертификаты в формате PKCS#10.

При необходимости АКС ФП запрашивает у АКС Банка xml-файлы с информацией, необходимой для изготовления ключей КК ФП и КО ФП. АКС Банка направляет запрошенную информацию в адрес АКС ФП по электронной почте.

6.4. АКС ФП сообщает АКС Банка по электронной почте выбранный способ идентификации ФП.

6.5. В случае прохождения идентификации ФП путем личного присутствия АКС ФП направляет на электронную почту АКС Банка файлы с запросами на сертификаты основного и резервного ключей КК ФП и/или КО ФП. АКС Банка согласовывает с АКС ФП адрес и время прибытия АКС ФП в Банк России для проведения дальнейших работ по созданию сертификатов и идентификации ФП.

В случае прохождения идентификации ФП без личного присутствия АКС ФП направляет через ЛК в адрес Департамента безопасности Банка России архив с файлами запросов на сертификаты основного и резервного ключей КК ФП и/или КО ФП, подписанный УКЭП ФП, с сопроводительным письмом. Допускается подписание архива с файлами запросов на сертификаты УКЭП ФП средствами ЛК.

6.6. В случае проведения идентификации путем личного присутствия АКС ФП прибывает в Банк России с документом, удостоверяющим личность. АКС Банка/работник подразделения Банка России проверяет полномочия АКС ФП в соответствии с доверенностью и, в случае успешной проверки, производит передачу АКС ФП файлов сертификатов основных и резервных ключей КК ФП и/или КО ФП «новой» серии. Передача файлов оформляется актом в произвольной форме.

6.7. В случае прохождения идентификации без личного присутствия файлы сертификатов основных и резервных ключей КК ФП и/или КО ФП направляются в адрес ФП через ЛК с дополнительным оповещением АКС ФП по электронной почте.

6.8. АКС Банка направляет в адрес ФП через ЛК файлы визуализации регистрационных карточек сертификатов ФП в формате «.pdf» с сопроводительным письмом. АКС ФП распечатывает в двух экземплярах файлы визуализации регистрационных карточек сертификатов КК ФП и/или КО ФП, оформляет их в соответствии с требованием раздела 12 настоящего Регламента. Первые экземпляры на бумажном носителе заверенных регистрационных карточек сертификатов остаются у ФП, вторые

экземпляры на бумажном носителе направляются ФП в подразделение Банка России, обслуживающее счет цифрового рубля ФП.

6.9. АКС Банка производит проверку регистрационных карточек сертификатов. В случае нахождения ошибок в оформлении регистрационных карточек сертификатов на электронную почту АКС ФП направляется соответствующее сообщение. До устранения замечаний дальнейшие работы не производятся. В случае успешной проверки АКС Банка направляет на электронную почту АКС ФП сообщение об успешном завершении создания сертификатов ФП, информацию о возможности ввода в действие ключей КК ФП и КО ФП «новой» серии, выводу из действия ключей КК ФП и КО ФП «текущей» серии (при необходимости).

7. Смена ключей ПУЦ ФП

7.1. Смену ключа ПУЦ ФП инициирует АКС ФП.

7.2. Смена ключа ПУЦ ФП по причине окончания первого периода использования ключа ПУЦ ФП должна быть инициирована АКС ФП не позднее чем за 2 месяца до окончания этого периода.

При необходимости АКС ФП запрашивает у АКС Банка xml-файл с информацией, необходимой для изготовления ключа ПУЦ ФП. АКС Банка направляет запрошенную информацию в адрес АКС ФП по электронной почте.

7.3. АКС ФП сообщает АКС Банка по электронной почте выбранный способ идентификации ФП.

7.4. В случае прохождения идентификации ФП путем личного присутствия АКС ФП направляет на электронную почту АКС Банка файл с запросом на сертификат ключа ПУЦ ФП. АКС Банка согласовывает с АКС ФП адрес и время прибытия АКС ФП в Банк России для проведения дальнейших работ по созданию сертификата и идентификации ФП.

В случае прохождения идентификации ФП без личного присутствия АКС ФП направляет через ЛК в адрес Департамента безопасности Банка

России архив с файлом запроса на сертификат ключа ПУЦ ФП, подписанный УКЭП ФП, с сопроводительным письмом. Допускается подписание архива с файлом запроса на сертификат УКЭП ФП средствами ЛК.

7.5. В случае проведения идентификации путем личного присутствия АКС ФП прибывает в Банк России с документом, удостоверяющим личность. АКС Банка/работник подразделения Банка России проверяет полномочия АКС ФП в соответствии с доверенностью и, в случае успешной проверки, производит передачу АКС ФП сертификата ПУЦ ФП «новой» серии. Передача файла оформляется актом в произвольной форме.

7.6. В случае прохождения идентификации без личного присутствия сертификат ПУЦ ФП «новой» серии направляется в адрес ФП через ЛК с дополнительным оповещением АКС ФП по электронной почте.

7.7. АКС Банка направляет в адрес ФП через ЛК файл визуализации регистрационной карточки сертификата ПУЦ ФП в формате «.pdf» с сопроводительным письмом. АКС ФП распечатывает в двух экземплярах файл визуализации регистрационной карточки сертификата ПУЦ ФП, оформляет их в соответствии с требованием раздела 12 настоящего Регламента. Первые экземпляры на бумажном носителе заверенных регистрационных карточек сертификатов остаются у ФП, вторые экземпляры на бумажном носителе направляются ФП в подразделение Банка России, обслуживающее счет цифрового рубля ФП.

7.8. Создание сертификатов, подписанных ключом ПУЦ ФП «новой» серии, до указания АКС Банка о возможности ввода в действие ключа ПУЦ ФП «новой» серии не допускается.

7.9. ФП выпускает САС ПУЦ ФП, подписывая его ключом ПУЦ «новой» серии в соответствии с требованиями раздела 4 настоящего Регламента. АКС ФП направляет файл с САС ПУЦ ФП в адрес АКС Банка по электронной почте.

7.10. АКС Банка направляет письмо на электронную почту АКС ФП с информацией о результате загрузки САС ПУЦ ФП в УЦ ПлЦР.

7.11. АКС Банка производит проверку регистрационной карточки сертификата ПУЦ ФП. В случае нахождения ошибок в оформлении регистрационной карточки сертификата на электронную почту АКС ФП направляется соответствующее сообщение. До устранения замечаний дальнейшие работы не производятся

7.12. В случае успешной проверки АКС Банка направляет на электронную почту АКС ФП соответствующее сообщение об успешном завершении работ по созданию сертификата ПУЦ ФП и возможности ввода его в действие.

7.13. ФП организует доведение сертификата ПУЦ ФП до пользователей, при необходимости.

7.14. После ввода в действие ключа ПУЦ ФП «новой» серии, ключ ПУЦ ФП предыдущей серии продолжает использоваться ФП до окончания своего срока действия для подписания САС (аннулирования сертификатов, подписанных данным ключом).

8. Смена ключей УЦ ПлЦР Банка России

8.1. АКС Банка направляет АКС ФП сообщение о проведении работ по смене ключа УЦ ПлЦР. В сообщении указывается номер «новой» серии ключа.

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

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

8.4. АКС ФП организует передачу сертификата УЦ ПлЦР «новой» серии и его САС пользователям ПлЦР, при необходимости.

8.5. АКС ФП направляет письмо АКС Банка по электронной почте с информацией о завершении работ, предписанных пунктом 8.3, настоящего Регламента.

9. Смена ключей компонентов ПлЦР

9.1. АКС Банка направляет АКС ФП по электронной почте сертификаты компонентов ПлЦР.

9.2. ФП осуществляет обработку поступивших от АКС Банка сертификатов, указанных в пункте 9.1.

9.3. АКС ФП направляет письмо АКС Банка по электронной почте с информацией о завершении работ, предписанных пунктом 9.2, настоящего Регламента.

10. Порядок действий в случае компрометации ключей ФП

10.1. В случае компрометации основного ключа КК/КО ФП и при наличии технической возможности АКС ФП готовит запрос на аннулирование сертификата основного ключа, сохраняет его в файл и направляет его АКС Банка России с использованием электронной почты, указывая причины и обстоятельства компрометации.

В случае компрометации основного ключа КК/КО ФП и при отсутствии технической возможности создания запроса на аннулирование сертификата ФП готовит уведомление о компрометации основного ключа (с указанием идентификатора скомпрометированного ключа и (или) серийного номера сертификата скомпрометированного ключа), подписанное руководителем ФП (либо лицом его замещающим или уполномоченным лицом), и направляет его в Департамент безопасности Банка России.

10.2. АКС ФП проводит действия по переходу на работу с резервным ключом – устанавливает в качестве рабочего сертификат резервного ключа, т.е. устанавливает СКЗИ в такой режим работы, при котором операции по

зашифрованию/расшифрованию или подписанию осуществляются с использованием резервного ключа КК/КО ФП.

10.3. С этого момента для работы используется резервный ключ КК/КО ФП, который переходит в статус основного.

10.4. АКС ФП проводит работы по изготовлению нового резервного ключа КК/КО ФП. Работы проводятся по аналогии с работами, описанными в разделе 3 настоящего Регламента в части ключей КК ФП и КО ФП.

10.5. В случае компрометации резервного ключа КК/КО проводятся работы, аналогичные работам, описанным в пункте 10.1 настоящего Регламента, с учетом того, что скомпрометирован резервный ключ КК/КО ФП. АКС ФП проводит работы по изготовлению нового резервного ключа КК/КО ФП. Работы проводятся по аналогии с работами, описанными в разделе 3 настоящего Регламента в части ключей КК ФП и КО ФП.

10.6. В случае компрометации основного и резервного ключей КК/КО, АКС ФП незамедлительно сообщает об этом АКС Банка по электронной почте, далее подготавливает уведомление о компрометации основного и резервного ключей КК/КО, подписанное руководителем ФП, и направляет его в Департамент безопасности Банка. Работа ФП с ПлЦР Банка России прекращается до изготовления и ввода в действие новых основного и резервного ключей КК/КО. Работы по изготовлению новых основного и резервного ключей производятся в соответствии с разделом 3 настоящего Регламента.

10.7. При компрометации действующего ключа ПУЦ ФП АКС ФП должен незамедлительно сообщить об этом АКС Банка по электронной почте.

10.8. ФП направляет в Департамент безопасности Банка России письмо за подписью руководителя с описанием ситуации. АКС Банка будут организованы работы по смене ключа ПУЦ ФП.

10.9. При компрометации ключа ПУЦ ФП, скомпрометированными считаются все сертификаты, подписанные ключом ПУЦ ФП «текущей»

серии. АКС ФП необходимо заново провести первичное изготовление ключа ПУЦ ФП (при необходимости) в соответствии с разделом 3 настоящего Регламента.

10.10. АКС Банка проводит мероприятия по аннулированию сертификатов скомпрометированных ключей и направляет в адрес ФП САС УЦ ПлЦР установленным порядком.

10.11. АКС ФП обрабатывает полученный файл с САС, о результатах сообщает АКС Банка по электронной почте.

11. Порядок уничтожения ключей

11.1. Выведенные из действия ключи уничтожаются ФП самостоятельно в соответствии с требованиями технической документации на используемое СКЗИ.

12. Порядок изготовления регистрационной карточки сертификата ФП

12.1. Регистрационная карточка сертификата должна содержать, в том числе:

- наименование организации владельца ключа сертификата;
- информацию, идентифицирующую ключ и соответствующий ему сертификат (идентификатор и (или) серийный номер сертификата);
- информацию о назначении ключа (область применения);
- даты начала и окончания действия ключа и соответствующего ему сертификата открытого ключа;
- значение открытого ключа в шестнадцатеричной системе счисления;
- алгоритм электронной подписи;
- фамилию и инициалы, должность и собственноручную подпись руководителя или АКС ФП, заверенную оттиском печати владельца ключа.

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

12.3. Регистрационная карточка сертификата каждого ключа изготавливается в двух экземплярах. Один экземпляр хранится в Банке России, другой – у ФП.

13. Порядок получения тестовой ключевой информации

13.1. Порядок получения тестовой ключевой информации для ФП аналогичен порядку получения промышленной ключевой информации, с учетом того, что печать, оформление, направление в Банк России экземпляров регистрационных карточек сертификатов ФП и идентификация ФП не производится. Взаимодействие между АКС Банка и АКС ФП происходит с использованием электронной почты. Информацию о наличии/отсутствии технической возможности создания ключей тестового ПУЦ ФП сроком действия 36 месяцев и их записи на используемые ФП ключевые носители, а также информацию об изменении данного статуса АКС ФП направляет АКС Банка с использованием электронной почты.