

**Акционерное общество
«Российский Сельскохозяйственный банк»
(АО «Россельхозбанк»)**

УТВЕРЖДЕН
решением Правления АО «Россельхозбанк»
(протокол от 28.12.2021 № 93)
введен в действие приказом АО «Россельхозбанк»
от 10.01.2022 № 2-ОД

**Регламент
Удостоверяющего центра АО «Россельхозбанк» № 133-Р**

ССП-владелец НД:	Департамент информационной безопасности (ДИБ)
Код и наименование процесса:	2.01.15.00.02. Обеспечение информационной безопасности
Код нормативного документа:	0-09/02
Номер версии:	01
Область применения:	ГО/ВСП Банка/РФ/ВСП РФ

Москва

Содержание

1. Термины, определения и сокращения.....	3
2. Нормативная база.....	8
3. Общие положения.....	9
4. Основные функции УЦ РСХБ	10
5. Условия конфиденциальности.....	11
6. Права и обязанности УЦ РСХБ	12
7. Права и обязанности Субъектов информационного обмена	14
8. Ответственность сторон	15
9. Сроки действия криптографических ключей и сертификатов ключей проверки электронной подписи	16
10. Регистрация Субъекта информационного обмена в реестре УЦ РСХБ.....	17
11. Создание сертификата ключа проверки электронной подписи	18
12. Аннулирование сертификата ключа проверки электронной подписи	20
13. Приостановление действия сертификата ключа проверки электронной подписи.....	22
14. Возобновление действия сертификата ключа проверки электронной подписи.....	23
15. Смена криптографических ключей Уполномоченного лица Банка	24
16. Смена криптографических ключей Субъекта информационного обмена	24
17. Порядок действий владельца сертификата ключа проверки электронной подписи при компрометации его ключа электронной подписи	25
18. Предоставление сервисов Службы актуальных статусов сертификатов и Службы штампов времени	25
19. Хранение материалов УЦ РСХБ	26
20. Порядок актуализации	27

Приложение:

1. Структура сертификата ключа проверки электронной подписи Уполномоченного лица АО «Россельхозбанк».
2. Структура списка аннулированных сертификатов ключей проверки электронной подписи Удостоверяющего центра АО «Россельхозбанк».
3. Структура сертификата ключа проверки электронной подписи Субъекта информационного обмена Удостоверяющего центра АО «Россельхозбанк».
4. Образец сертификата ключа проверки электронной подписи, выпущенного Удостоверяющим центром АО «Россельхозбанк».
5. Положение о разборе конфликтных ситуаций.
6. Список поддерживаемых Удостоверяющим центром АО «Россельхозбанк» ключевых носителей.
7. Заявление на регистрацию Субъекта информационного обмена.
8. Расписка Субъекта информационного обмена о получении временных ключей ЭП, временного сертификата ключа проверки ЭП в электронной форме, временного сертификата ключа проверки ЭП в виде документа на бумажном носителе.
9. Запрос на изготовление сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра АО «Россельхозбанк».
10. Запрос на аннулирование сертификата ключа проверки электронной подписи Субъекта информационного обмена.
11. Запрос на приостановление действия сертификата ключа проверки электронной подписи Субъекта информационного обмена.
12. Запрос на возобновление действия сертификата ключа проверки электронной подписи Субъекта информационного обмена.
13. Заявление на проверку подлинности электронной подписи в электронном документе.
14. Заявление на повторное изготовление временного сертификата ключа проверки электронной подписи.
15. Заявления о предоставлении сертификата ключа проверки электронной подписи на бумажном носителе.
16. Перечень объектных идентификаторов (OID), определяющих области применения электронной подписи.

1. Термины, определения и сокращения

Администратор Центра регистрации – работник головного офиса Банка, официально назначенный и уполномоченный на рассмотрение и обработку запросов на выдачу, аннулирование, приостановление действия и возобновление действия сертификатов ключей проверки электронной подписи;

Администратор по разбору конфликтных ситуаций – работник головного офиса Банка, официально назначенный и уполномоченный на формирование экспертной комиссии для проведения технической экспертизы по проверке подлинности ЭП в электронном документе по заявлению одного из Субъектов информационного обмена;

Банк – АО «Россельхозбанк»;

владелец сертификата ключа проверки ЭП – Субъект информационного обмена, которому в установленном настоящим Регламентом порядке УЦ РСХБ выдан сертификат ключа проверки ЭП;

внеплановая смена ключей ЭП – смена ключевой пары, вызванная компрометацией ключа ЭП, а также в случае выхода из строя ключевого носителя;

временная ключевая пара и временный сертификат ключа проверки ЭП – ключевая пара, а также связанный с данной ключевой парой сертификат ключа проверки ЭП, предназначенные исключительно для:

– обеспечения аутентификации зарегистрированного пользователя УЦ РСХБ при использовании программного обеспечения, предоставляемого Банком, для формирования запроса на выдачу сертификата ключа проверки ЭП Субъекта информационного обмена в электронном виде.

ВСП – внутреннее структурное подразделение филиала/Банка;

заявитель - коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица (далее - нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата;

заявление на регистрацию Субъекта информационного обмена (заявление на регистрацию СИО) – документ, выполненный по форме Приложения 7 к настоящему Регламенту, на основании которого осуществляется регистрация Субъекта информационного обмена в реестре УЦ РСХБ;

информационная система (далее – ИС) – автоматизированная банковская и/или информационная система, введенная в промышленную или опытную эксплуатацию, с использованием которой происходит осуществление защищенного электронного документооборота и обмен подписанными ЭП электронными документами с другими Субъектами информационного обмена с использованием услуг УЦ РСХБ;

инфраструктура открытых ключей (Public Key Infrastructure, PKI) – интегрированный набор служб и приложений, основанных на технологии асимметричной криптографии, которая обеспечивает функции управления ключами проверки ЭП и сертификатами ключей проверки ЭП Субъектов информационного обмена;

Клиент – юридическое лицо /индивидуальный предприниматель/физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, а также физическое лицо, уполномоченное на подписание ЭП документов от имени указанных лиц;

ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее – проверка ЭП);

ключ ЭП – уникальная последовательность символов, предназначенная для создания ЭП;

ключевая пара (криптографические ключи) – ключ ЭП и соответствующий ему ключ проверки ЭП;

ключевая информация – ключ ЭП, ключ проверки ЭП, Сертификат ключа проверки электронной подписи;

ключевой носитель – отчуждаемый носитель информации, предназначенный для размещения ключевой информации, используемой для выполнения криптографических процедур шифрования и расшифрования, формирования ЭП. Список поддерживаемых УЦ РСХБ ключевых носителей информации приведен в Приложении 6 к настоящему Регламенту;

Комплект документов – документы, устанавливающие договорные отношения Банка с Клиентами при осуществлении защищенного юридически значимого электронного документооборота и обмена информацией (в случае, если при защите указанного документооборота/обмена информацией предусматривается применение услуг УЦ РСХБ), к условиям которых Клиент присоединяется в порядке, предусмотренном соответствующим договором (соглашением), предусматривающим использование системы электронного документооборота, и соглашается с ними в целом;

компрометация ключа (ключевой информации) – установленный факт раскрытия закрытой ключевой информации (ключа ЭП) или подозрение на раскрытие закрытой ключевой информации; утрата доверия к тому, что используемая ключевая информация обеспечивает подлинность, защищенность и безопасность информации.

К фактам, которые могут рассматриваться как компрометация (или подозрение на компрометацию) ключа ЭП, относятся следующие события:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим их обнаружением;
- увольнение работника, имевшего доступ к ключу ЭП и (или) к ключевому носителю, на который записан указанный ключ ЭП;
- возникновение подозрений на утечку конфиденциальной информации или ее искажение;
- нарушение целостности упаковки ключевых носителей и (или) печати на хранилище, где хранились эти носители.

Первые три события должны трактоваться как безусловная компрометация ключа ЭП, остальные - как подозрение на компрометацию ключа ЭП;

конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

конфликтная ситуация – ситуация, при которой у Субъектов информационного обмена возникает необходимость разрешить вопросы признания или непризнания авторства, целостности и/или подлинности электронных документов, преобразованных с использованием средств ЭП. Положение о разборе конфликтных ситуаций приведено в Приложении 5 к настоящему Регламенту;

корректный электронный документ – электронный документ, подписанный усиленной неквалифицированной ЭП, и признанный равнозначным документу на бумажном

носителе, подписанному собственноручной подписью, при положительном результате проверки ЭП с использованием сертифицированных¹ средств ЭП;

несанкционированный доступ к информации – доступ к информации, нарушающий установленные правила разграничения доступа в результате случайных или преднамеренных действий Субъектов информационного обмена или других субъектов, с использованием штатных аппаратных, аппаратно-программных, программных средств автоматизированной системы;

обработка запроса на выдачу, аннулирование, приостановление действия или возобновление действия сертификата ключа проверки электронной подписи – совокупность действий работников УЦ РСХБ по созданию сертификата ключа проверки ЭП и занесению о нем сведений в реестры УЦ РСХБ, занесению сведений об аннулировании сертификата ключа проверки ЭП, приостановлении/возобновлении действия сертификата ключа проверки ЭП в реестры УЦ РСХБ и формированию и публикации списка аннулированных сертификатов ключей проверки ЭП, а также уведомлению владельца сертификата ключа проверки ЭП о создании, аннулировании, приостановлении или возобновлении действия сертификата ключа проверки ЭП в порядке, установленном настоящим Регламентом;

объектный идентификатор – это атрибут сертификата ключа проверки электронной подписи, определяющий отношения, при осуществлении которых электронный документ, подписанный электронной подписью, будет иметь юридическое значение.

Оператор Центра регистрации (Оператор ЦР) – работник головного офиса/регионального филиала Банка, официально назначенный и уполномоченный на проведение работ по регистрации Субъектов информационного обмена в реестре УЦ РСХБ, а также создание временных ключей ЭП и временных сертификатов ключей проверки ЭП при выполнении процедуры регистрации Субъектов информационного обмена;

ответственный работник АО «Россельхозбанк» (ОР) – операционный работник фронт-офиса, уполномоченный на проведение идентификации Субъектов информационного обмена, а также на прием заявлений пользователей на осуществление действий по регистрации и управлению сертификатами ключей проверки ЭП, полученных в УЦ РСХБ;

Online Certificate Status Protocol (OCSP) – протокол установления статуса сертификата ключа проверки электронной подписи, реализованный в соответствии со стандартом RFC 6960 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP»;

плановая смена ключей ЭП – смена ключевой пары с установленной настоящим Регламентом периодичностью, которая не вызвана компрометацией ключа ЭП;

подтверждение владения ключом ЭП – получение УЦ РСХБ доказательства того, что Субъект информационного обмена владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному Субъектом информационного обмена в запросе на выдачу сертификата ключа проверки ЭП;

рабочий день ОР – период обслуживания Клиентов в соответствии с режимом работы подразделения Банка, в которое обратился Клиент;

рабочий день УЦ РСХБ (далее - рабочий день) – период с 09 часов 00 минут до 18 часов 00 минут с понедельника по четверг и с 09 часов 00 минут до 16 часов 45 минут в пятницу по времени часовой зоны г. Москвы за исключением праздничных нерабочих дней согласно законодательству Российской Федерации;

рассмотрение запроса на аннулирование сертификата ключа проверки ЭП, приостановление/возобновление действия сертификата ключа проверки ЭП – принятие

¹ Соответствующих требованиям к средствам ЭП, утвержденным Приказом ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

Администратором ЦР решения об осуществлении обработки запроса на основе предоставленных владельцем сертификата ключа проверки ЭП документов;

регистрация Субъектов информационного обмена – внесение в реестры УЦ РСХБ регистрационной информации о Субъекте информационного обмена;

Регламент – Регламент Удостоверяющего центра АО «Россельхозбанк» № ____ -Р;

реестры УЦ РСХБ – набор документов УЦ РСХБ в электронной и/или бумажной форме, включающий следующую информацию:

- реестр запросов на регистрацию Субъектов информационного обмена в УЦ РСХБ;
- реестр зарегистрированных Субъектов информационного обмена;
- реестр запросов на выдачу сертификатов ключей проверки ЭП;
- реестр запросов на аннулирование сертификатов ключей проверки ЭП;
- реестр запросов на приостановление/возобновление действия сертификатов ключей проверки ЭП;

- реестр выданных и аннулированных сертификатов ключей проверки ЭП;

- реестр изготовленных списков аннулированных сертификатов;

сертификат ключа проверки ЭП – электронный документ или документ на бумажном носителе, выданные УЦ РСХБ Субъектам информационного обмена и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Сертификат ключа проверки ЭП содержит следующие сведения:

- уникальный регистрационный номер сертификата ключа проверки ЭП;
- даты начала и окончания срока действия сертификата ключа проверки ЭП;
- фамилию, имя и отчество владельца сертификата ключа проверки ЭП – для физических лиц, наименование и место нахождения – для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;

- значение ключа проверки ЭП;

- наименование средств ЭП, которые использованы для создания ключа ЭП, ключа проверки ЭП и сертификата;

- наименование УЦ РСХБ, выдавшего сертификат ключа проверки ЭП;

- сведения об области применения ЭП².

Структура сертификата ключа проверки электронной подписи Уполномоченного лица АО «Россельхозбанк» и структура сертификата ключа проверки электронной подписи Субъекта информационного обмена Удостоверяющего центра АО «Россельхозбанк» приведены в Приложении 1 и Приложении 3 к настоящему Регламенту.

Образец сертификата ключа проверки ЭП, выданного УЦ РСХБ Субъекту информационного обмена, в виде документа на бумажном носителе приведен в Приложении 4 к настоящему Регламенту;

система Lotus Notes – автоматизированная система коллективной работы Lotus Notes;

Служба актуальных статусов сертификатов – сервис УЦ РСХБ, построенный на базе протокола OCSP, с использованием которого подписываются ЭП и предоставляются Клиентам электронные ответы, содержащие информацию о статусе сертификатов ключа проверки ЭП, выданных УЦ РСХБ;

Служба штампов времени – сервис УЦ РСХБ, построенный на базе протокола TSP, с использованием которого подписываются ЭП и предоставляются Клиентам штампы времени;

список аннулированных сертификатов (CRL) – список сертификатов ключей проверки ЭП, которые были аннулированы или действие которых на определенный период времени было приостановлено. Время формирования CRL определяется по значению поля «Действителен с» CRL. Структура списка аннулированных сертификатов ключей проверки

² Приложение 16 к настоящему Регламенту.

электронной подписи Удостоверяющего центра АО «Россельхозбанк» приведена в Приложении 2 к настоящему Регламенту;

средство ЭП – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций:

- создание ЭП;
- проверка ЭП;
- создание ключа ЭП и ключа проверки ЭП.

Для предоставления криптографических сервисов УЦ РСХБ применяется сертифицированное программное средство криптографической защиты информации КриптоПро CSP с поддержкой криптографических алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 вариантов исполнения 1-Base, 2-Base в соответствии с требованиями формуляров и эксплуатационной документации;

Стандарт RFC (Request for Comments) – разработанный под эгидой международной профессиональной организации (ISOC – Internet Society) документ из серии пронумерованных информационных документов, содержащий технические спецификации и стандарты. УЦ РСХБ обеспечивает работу сервисов, реализованных в соответствии со следующими стандартами RFC:

– RFC 6960 – стандарт RFC 6960 Online Certificate Status Protocol (OCSP), определяющий протокол установления статуса сертификата ключа проверки электронной подписи;

– RFC 3161 – стандарт RFC 3161 Time-Stamp Protocol (TSP), определяющий протокол предоставления штампа времени;

Стандарты асимметричной криптографии с открытым ключом (Public Key Cryptography Standarts - PKCS) – разработанные компанией RSA Security стандарты, определяющие формат и синтаксис передаваемых криптографических сообщений. УЦ РСХБ осуществляет свою работу в соответствии со следующими стандартами PKCS:

– PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений, тип данных PKCS#7 Signed – подписанные данные;

– PKCS#10 – стандарт, определяющий формат и синтаксис запроса на выдачу сертификата ключа проверки ЭП;

– XMLDSIG - стандарт, определяющий формат и синтаксис ЭП XML сообщений;

страховой номер индивидуального лицевого счета (далее - СНИЛС) – уникальный номер индивидуального лицевого счёта застрахованного лица в системе обязательного пенсионного страхования;

Субъект информационного обмена – физическое лицо, уполномоченное на осуществление юридически значимого защищенного электронного обмена с использованием ЭП в соответствии с Комплектом документов, определяющим взаимоотношения сторон при указанном обмене и хранении электронных документов с использованием ИС Банка;

Time-Stamp Protocol (TSP) – протокол предоставления штампа времени, реализованный в соответствии со стандартом RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)»;

Удостоверяющий центр Банка (УЦ РСХБ) – подразделение АО «Россельхозбанк», осуществляющее свою деятельность в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и являющееся распорядителем комплекса программно-технических средств, предназначенного для:

- обеспечения функционирования PKI Банка;
- осуществления функций по созданию и выдаче сертификатов ключей проверки электронных подписей;
- осуществления иных функций, предусмотренных настоящим Регламентом.

Удостоверяющий центр АО «Россельхозбанк» не относится к аккредитованным удостоверяющим центрам в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об

электронной подписи» и сертификаты ключей проверки ЭП, выданные УЦ РСХБ, не относятся к квалифицированным сертификатам ключей проверки ЭП.

Электронная подпись, удовлетворяющая указанным выше требованиям, созданная с применением сертификата ключа проверки ЭП, выданного УЦ РСХБ, относится к усиленным неквалифицированным ЭП;

Уполномоченное лицо Банка – должностное лицо Банка, официально назначенное и уполномоченное подписывать собственноручной подписью или ЭП сертификаты ключей проверки ЭП и CRL, выдаваемые и публикуемые УЦ РСХБ;

Уполномоченное должностное лицо – представитель Клиента - руководитель организации или иное лицо, уполномоченное в соответствии с Комплектом документов на подачу запросов на аннулирование сертификатов ключей проверки ЭП Субъектов информационного обмена, также представляющих отмеченного Клиента Банка;

усиленная неквалифицированная ЭП – электронная подпись, которая:

– получена в результате криптографического преобразования информации с использованием ключа ЭП;

– позволяет определить лицо, подписавшее электронный документ;

– позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

– создана с использованием средств электронной подписи;

участники электронного взаимодействия – Банк и его Клиенты, осуществляющие обмен информацией в электронной форме;

фронт-офис – отдел/служба/специалист продаж и обслуживания либо отдел/служба/специалист продаж и обслуживания юридических лиц филиала, ВСП Банка/филиала Банка;

Центр регистрации (ЦР) – логический компонент в составе комплекса программно-технических средств УЦ РСХБ;

штамп времени электронного документа (штамп времени) – электронный документ, подписанный ЭП и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе;

электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

ЭП (электронная подпись) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В рамках настоящего Регламента под электронной подписью понимается УНЭП, выданная УЦ РСХБ.

2. Нормативная база

Настоящий Регламент разработан в соответствии с требованиями законодательных и нормативных актов Российской Федерации, руководящих документов и методических рекомендаций ФСБ России:

- Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Перечня сведений конфиденциального характера (утвержден Указом Президента Российской Федерации от 06.03.1997 № 188);

- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требованиям к средствам удостоверяющего центра»;
- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) (утверждено приказом ФСБ России от 09.02.2005 № 66);
- Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утверждена приказом Федерального агентства правительственной связи при Президенте Российской Федерации от 13.06.2001 № 152).

3. Общие положения

3.1. Настоящий Регламент разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров и является основополагающим документом в области использования электронных подписей при совершении гражданско-правовых сделок и при совершении иных юридически значимых действий.

3.2. УЦ РСХБ осуществляет свою деятельность на территории Российской Федерации по созданию и выдаче неквалифицированных сертификатов ключей проверки электронных подписей на основании имеющейся у АО «Россельхозбанк» лицензии³.

3.3. В настоящем Регламенте определены механизмы и условия предоставления и правила пользования услугами УЦ РСХБ, форматы данных и основные организационно-технические мероприятия, необходимые для обеспечения работы УЦ РСХБ и пользователей его услуг.

Настоящий Регламент определяет взаимоотношения Банка с пользователями услуг УЦ РСХБ, включая права, обязанности и ответственность сторон, в рамках предоставления указанных услуг.

В рамках договорных отношений Банка с клиентами и/или партнерами (далее - Клиенты), связанных с осуществлением защищенного юридически значимого электронного документооборота и обменом информацией (в случае, если при защите указанного документооборота/обмена информацией предусматривается применение услуг УЦ РСХБ), Регламент является частью Комплекта документов, устанавливающих договорные отношения Банка с Клиентами при осуществлении защищенного юридически значимого электронного документооборота и обмена информацией, к условиям которых Клиент присоединяется в порядке, предусмотренном соответствующим договором (соглашением), предусматривающим использование системы электронного документооборота, и соглашается с ними в целом.

3.4. Настоящий Регламент обязателен для исполнения после подписания пользователями услуг Комплекта документов в течение срока договорных отношений.

³ Лицензия на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) (выдана Центром по лицензированию, сертификации и защите государственной тайны ФСБ России от 05.02.2019 рег. № 17078 Н).

В случае внесения изменений в настоящий Регламент или прекращения его действия, соответствующая информация размещается на сайте Банка. Актуальная редакция настоящего Регламента размещается на официальном сайте Банка <https://www.rshb.ru> в разделе Информация об услугах - Удостоверяющий центр.

3.5. Сторонами настоящего Регламента являются:

- АО «Россельхозбанк»;
- пользователи услуг – Субъекты информационного обмена⁴, уполномоченные в соответствии с Комплектом документов осуществлять обмен электронными документами.

3.6. Настоящий Регламент определяет обязательства сторон, а также служит средством официального уведомления и информирования указанных сторон обо всех типах взаимоотношений, возникающих в процессе оказания и использования услуг УЦ РСХБ.

3.7. Настоящий Регламент распространяется в следующих формах:

- в электронной форме в виде файла формата PDF на официальном сайте Банка <https://www.rshb.ru>;
- в форме документа на бумажном носителе с Комплектом документов.

3.8. Адрес Удостоверяющего центра Банка для переписки:

119034, Москва, Гагаринский переулок, д. 3.

3.9. Прекращение деятельности УЦ РСХБ:

3.9.1. Деятельность УЦ РСХБ может быть прекращена в порядке, установленном действующим законодательством Российской Федерации. При этом информация, внесенная в реестр сертификатов ключей проверки электронных подписей, выданных УЦ РСХБ, уничтожается или передается лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность, в соответствии с порядком, установленным действующим законодательством Российской Федерации.

3.9.2. Официальное уведомление о прекращении деятельности УЦ РСХБ и действия настоящего Регламента осуществляется путем публикации текста официального уведомления на официальном сайте Банка <https://www.rshb.ru>.

Официальное уведомление о прекращении деятельности УЦ РСХБ направляется также в письменном виде владельцам сертификатов ключей проверки электронных подписей, которые выданы УЦ РСХБ и срок действия которых не истек, ОР на адреса Клиента, определенные для указанных целей в Комплекте документов, не менее чем за один месяц до даты прекращения деятельности УЦ РСХБ.

4. Основные функции УЦ РСХБ

4.1. УЦ РСХБ предназначен для оказания услуг по созданию, публикации и аннулированию сертификатов ключей проверки ЭП, а также для предоставления иных услуг, соответствующих положениям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». В рамках своей деятельности УЦ РСХБ осуществляет следующие функции:

- регистрирует Субъектов информационного обмена;
- создает и выдает сертификаты ключей проверки ЭП по обращению заявителей;
- устанавливает сроки действия сертификатов ключей проверки ЭП;
- аннулирует выданные УЦ РСХБ сертификаты ключей проверки ЭП Субъектов информационного обмена;
- приостанавливает и возобновляет действие выданных УЦ РСХБ сертификатов ключей проверки ЭП Субъектов информационного обмена по обращениям их владельцев;
- выдает по обращению заявителя средства ЭП, обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП заявителем;

⁴ Информационный обмен осуществляется между Клиентами/между Клиентом и Банком.

- ведет реестр выданных и аннулированных УЦ РСХБ сертификатов ключей проверки ЭП, в том числе включающий в себя информацию, содержащуюся в выданных УЦ РСХБ сертификатах ключей проверки ЭП, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки ЭП и об основаниях таких прекращения или аннулирования;

- устанавливает порядок ведения реестра сертификатов ключей проверки ЭП и порядок доступа к нему, а также обеспечивает доступ участников электронного взаимодействия к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;

- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей и записывает их на ключевой носитель;

- проверяет уникальность ключей проверки ЭП в реестре сертификатов ключей проверки ЭП;

- устанавливает порядок проверки подлинности электронной подписи;

- изготавливает и публикует актуальный CRL, обеспечивает возможность свободного доступа участников электронного взаимодействия к CRL;

- осуществляет по обращениям участников электронного взаимодействия процедуру разбора конфликтных ситуаций, включающую проверку подлинности электронных подписей на основании Заявления на проверку подлинности электронной подписи в электронном документе⁵;

- предъявляет требования по обеспечению информационной безопасности при использовании средств ЭП в процессе осуществления юридически значимого электронного документооборота между Клиентом и Банком.

4.2. Порядок проверки подлинности электронной подписи состоит в проверке одновременного соблюдения следующих условий:

- сертификат ключа проверки ЭП действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата ключа проверки ЭП, если момент подписания документа не определен;

- имеется положительный результат проверки принадлежности владельцу сертификата ключа проверки ЭП, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания.

- ЭП используется в отношениях, определенных областями действия, указанными в сертификате ключа проверки ЭП лица, подписывающего электронный документ.

5. Условия конфиденциальности

5.1. Конфиденциальная информация:

5.1.1. Ключ ЭП, связанный с сертификатом ключа проверки ЭП Субъекта информационного обмена, является конфиденциальной информацией данного Субъекта информационного обмена и относится к служебной и коммерческой тайне.

УЦ РСХБ не осуществляет хранение ключей ЭП Субъектов информационного обмена, созданных по их заявлениям.

5.1.2. Реестры УЦ РСХБ, за исключением Реестра созданных и аннулированных сертификатов ключей проверки ЭП Субъектов информационного обмена, являются конфиденциальной информацией УЦ РСХБ и относятся к служебной и коммерческой тайне.

5.1.3. Отчет о проведении технической экспертизы по проверке подлинности ЭП в электронном документе, выполненной по заявлению Субъекта информационного обмена, является конфиденциальной информацией УЦ РСХБ.

⁵ Приложение 13 к настоящему Регламенту.

5.1.4. Персональные данные Субъектов информационного обмена и информация об организации, от лица которой действуют Субъекты информационного обмена, ставшая известной УЦ РСХБ в силу его деятельности и не подлежащая включению в сертификаты ключа проверки ЭП, являются конфиденциальной информацией.

5.2. Информация, не относящаяся к конфиденциальной информации:

5.2.1. Информация, не относящаяся к конфиденциальной информации, в соответствии с законодательством Российской Федерации, считается открытой информацией.

5.2.2. Настоящий Регламент не относится к конфиденциальной информации.

5.2.3. Сведения, включаемые в сертификаты ключей проверки ЭП и CRL, издаваемые УЦ РСХБ, не относятся к конфиденциальной информации.

5.2.4. Персональные данные, включаемые в сертификаты ключей проверки ЭП, выдаваемые УЦ РСХБ, относятся к общедоступным персональным данным.

5.2.5. Открытая информация может публиковаться по решению Банка. Место, способ и время публикации открытой информации определяются Банком.

5.3. Предоставление конфиденциальной информации УЦ РСХБ:

5.3.1. УЦ РСХБ имеет право раскрывать конфиденциальную информацию третьим лицам исключительно в порядке и случаях, установленных законодательством Российской Федерации и Комплектом документов.

6. Права и обязанности УЦ РСХБ

6.1. УЦ РСХБ обязан:

6.1.1. Использовать для создания ключа ЭП Уполномоченного лица Банка и формирования ЭП исключительно сертифицированные ФСБ России средства ЭП.

6.1.2. Использовать ключ ЭП Уполномоченного лица Банка исключительно для подписи выдаваемых УЦ РСХБ сертификатов ключей проверки ЭП и публикуемых CRL.

6.1.3. Принимать меры по защите ключа ЭП Уполномоченного лица Банка от несанкционированного доступа.

6.1.4. Использовать для создания ключей Субъектов информационного обмена исключительно сертифицированные ФСБ России средства ЭП.

6.1.5. Обеспечивать уникальность серийных номеров создаваемых сертификатов ключей проверки ЭП Субъектов информационного обмена.

6.1.6. Проверять уникальность значений ключей проверки ЭП в созданных сертификатах ключей проверки ЭП Субъектов информационного обмена.

6.1.7. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

6.1.8. Предоставлять безвозмездно Субъекту информационного обмена по его обращению доступ к информации, содержащейся в Реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.

6.1.9. Соблюдать сроки аннулирования сертификатов ключей проверки ЭП Субъектов информационного обмена.

6.1.10. Осуществлять регистрацию Субъектов информационного обмена на основании заявлений на регистрацию Субъекта информационного обмена, в соответствии с порядком, определенным настоящим Регламентом.

6.1.11. Обеспечивать занесение регистрационной информации Субъекта информационного обмена в реестр зарегистрированных Субъектов информационного обмена и обеспечивать уникальность регистрационной информации, используемой для идентификации владельцев сертификатов ключей проверки ЭП.

6.1.12. Обеспечивать конфиденциальность регистрационной информации Субъектов информационного обмена, за исключением информации, заносимой в выдаваемые УЦ РСХБ сертификаты ключей проверки ЭП.

6.1.13. Осуществлять создание сертификатов ключей проверки ЭП Субъектов информационного обмена в соответствии с порядком, определенным настоящим Регламентом.

6.1.14. Обеспечивать внесение информации о созданном сертификате ключа проверки ЭП Субъекта информационного обмена в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата.

6.1.15. Аннулировать сертификат ключа проверки ЭП Субъекта информационного обмена путем внесения записи о его аннулировании в реестр сертификатов и в CRL с указанием даты, времени внесения и причины аннулирования не позднее 1 (одного) рабочего дня УЦ РСХБ, следующего за рабочим днем, в течение которого запрос на аннулирование указанного сертификата ключа проверки ЭП был подан в УЦ РСХБ, в порядке, предусмотренном настоящим Регламентом.

6.1.16. Приостанавливать действие сертификата ключа проверки ЭП Субъекта информационного обмена и заносить сведения об отмеченном сертификате в CRL с указанием даты, времени внесения, срока и причины приостановления его действия не позднее 1 (одного) рабочего дня УЦ РСХБ, следующего за рабочим днем, в течение которого запрос на приостановление действия указанного сертификата был подан в УЦ РСХБ, в порядке, предусмотренном настоящим Регламентом.

6.1.17. Возобновлять действие сертификата ключа проверки ЭП Субъекта информационного обмена (в случае поступления заявления в период срока, на который действие сертификата было приостановлено) не позднее 1 (одного) рабочего дня УЦ РСХБ, следующего за рабочим днем, в течение которого запрос на возобновление действия указанного сертификата был подан в УЦ РСХБ, в порядке, предусмотренном настоящим Регламентом.

6.1.18. Аннулировать сертификат ключа проверки ЭП в случае, если истек установленный срок, на который действие данного сертификата было приостановлено, а запрос на возобновление его действия от владельца сертификата ключа проверки ЭП не поступил.

6.1.19. Уведомлять владельца сертификата ключа проверки ЭП о фактах аннулирования, приостановления или возобновления действия принадлежащего ему сертификата ключа проверки ЭП в порядке, предусмотренном настоящим Регламентом.

6.1.20. Обеспечивать сохранность и контроль доступа к конфиденциальной информации в соответствии с действующими нормативными актами Российской Федерации.

6.1.21. Гарантировать конфиденциальность сведений, полученных в связи с исполнением своих обязательств по настоящему Регламенту, в течение срока хранения документов, установленного архивным деломпроизводством.

6.1.22. Поддерживать во всех технических и программных средствах УЦ РСХБ, единое системное время, соответствующее времени часовой зоны г. Москвы, с точностью до 1 минуты.

6.2. УЦ РСХБ имеет право:

6.2.1. Наделить третьих лиц полномочиями по созданию и выдаче сертификатов ключей проверки электронных подписей от имени УЦ РСХБ, подписываемых электронной подписью, основанной на сертификате ключа проверки ЭП, выданном такому доверенному лицу УЦ РСХБ.

6.2.2. Отказать в предоставлении услуг по регистрации Субъекта информационного обмена в УЦ РСХБ в случае нарушения указанным Субъектом информационного обмена требований настоящего Регламента, с указанием причин отказа.

6.2.3. Отказать в предоставлении услуг по созданию ключей ЭП и ключей проверки ЭП и (или) созданию сертификата ключа проверки ЭП Субъекту информационного обмена в

случае нарушения указанным Субъектом информационного обмена требований настоящего Регламента, с указанием причин отказа.

6.2.4. Отказать Субъекту информационного обмена в предоставлении услуг по созданию сертификата ключа проверки ЭП в случае, если использованное для формирования запроса на выдачу сертификата ключа проверки ЭП средство ЭП не поддерживается УЦ РСХБ.

6.2.5. Отказать владельцу сертификата ключа проверки ЭП в аннулировании сертификата ключа проверки ЭП в случае, если истек установленный срок действия ключа ЭП, соответствующего указанному сертификату ключа проверки ЭП.

6.2.6. Отказать владельцу сертификата ключа проверки ЭП в приостановлении действия сертификата ключа проверки ЭП в случае, если истек установленный срок действия ключа ЭП, соответствующего указанному сертификату ключа проверки ЭП.

6.2.7. Отказать владельцу сертификата ключа проверки ЭП в возобновлении действия сертификата ключа проверки ЭП в случае, если истек установленный срок действия ключа ЭП, соответствующего указанному сертификату ключа проверки ЭП.

6.2.8. Аннулировать сертификат ключа проверки ЭП Уполномоченного лица Банка, Субъектов информационного обмена в случае установленного факта компрометации соответствующего ключа ЭП, в том числе и без соответствующего заявления со стороны владельца сертификата ключа проверки ЭП, в случае, если УЦ РСХБ стало достоверно известно о прекращении действия документа, на основании которого выдан сертификат ключа проверки ЭП, а также в установленных законодательством Российской Федерации случаях с последующим его уведомлением о факте и причине аннулирования.

6.2.9. Предоставлять услуги сервисов Службы актуальных статусов сертификатов и Службы штампов времени.

7. Права и обязанности Субъектов информационного обмена

7.1. Права Субъекта информационного обмена:

7.1.1. Применять ключи ЭП и сертификаты ключей проверки ЭП (выданные УЦ РСХБ), владельцем которых указанный Субъект информационного обмена является, для формирования ЭП под электронными документами в соответствии с содержащимися в сертификате ключа проверки ЭП сведениями об отношениях, при осуществлении которых электронный документ будет иметь юридическое значение.

7.1.2. Для сертификата ключа проверки ЭП, выданного в форме электронного документа, получить также копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную Уполномоченным лицом Банка.

7.1.3. Получать сертификат ключа проверки ЭП Уполномоченного лица Банка и использовать его для проверки ЭП Уполномоченного лица Банка в сертификатах ключа проверки ЭП, выданных УЦ РСХБ другим Субъектам информационного обмена.

7.1.4. Применять сертификат ключа проверки ЭП другого Субъекта информационного обмена, выданный УЦ РСХБ, для проверки ЭП электронных документов в соответствии со сведениями, указанными в сертификате ключа проверки ЭП.

7.1.5. Получать актуальный CRL УЦ РСХБ и применять его для проверки статуса сертификатов ключей проверки ЭП Субъектов информационного обмена и для проверки ЭП электронных документов.

7.1.6. Обращаться в порядке, предусмотренном настоящим Регламентом, в УЦ РСХБ для проверки подлинности ЭП в электронных документах, подписанных другими Субъектами информационного обмена с использованием сертификатов ключей проверки ЭП, выданных УЦ РСХБ.

7.1.7. Обращаться в порядке, предусмотренном настоящим Регламентом, в УЦ РСХБ для аннулирования сертификата ключа проверки ЭП, в течение срока действия данного сертификата ключа проверки ЭП.

7.1.8. Обращаться в порядке, предусмотренном настоящим Регламентом, в УЦ РСХБ для приостановления действия сертификата ключа проверки ЭП, владельцем которого он является, в течение срока действия данного сертификата ключа проверки ЭП.

7.1.9. Обращаться в порядке, предусмотренном настоящим Регламентом, в УЦ РСХБ для возобновления действия сертификата ключа проверки ЭП, владельцем которого он является, в течение срока действия ключа ЭП, связанного с данным сертификатом ключа проверки ЭП, и срока, на который действие сертификата ключа проверки ЭП было приостановлено.

7.1.10. Получать услуги сервисов Службы актуальных статусов сертификатов⁶ и Службы штампов времени⁷.

7.2. Обязанности Субъекта информационного обмена:

7.2.1. Соблюдать условия и порядок использования ключей ЭП и средств ЭП.

7.2.2. Обеспечивать конфиденциальность своего ключа ЭП, принимать все возможные меры для предотвращения утраты, раскрытия, искажения и несанкционированного использования ключа ЭП.

7.2.3. Применять для формирования ЭП только действующий не скомпрометированный ключ ЭП.

7.2.4. Не применять свой ключ ЭП, если стало известно или имеются подозрения, что этот ключ ЭП используется или использовался ранее другими лицами.

7.2.5. Немедленно обратиться в порядке, предусмотренном настоящим Регламентом, в УЦ РСХБ с запросом на аннулирование своего сертификата ключа проверки ЭП при наличии оснований полагать, что ключ ЭП скомпрометирован.

7.2.6. Не использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, запрос на аннулирование которого подан в УЦ РСХБ, с момента подачи запроса на аннулирование сертификата ключа проверки ЭП Субъекта информационного обмена в УЦ РСХБ.

7.2.7. Не использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, запрос на приостановление действия которого подан в УЦ РСХБ, с момента подачи запроса на приостановление действия сертификата ключа проверки ЭП Субъекта информационного обмена в УЦ РСХБ.

7.2.8. Не использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, который аннулирован или действие которого приостановлено. Использование аннулированного сертификата ключа проверки ЭП или сертификата ключа проверки ЭП, действие которого приостановлено, не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием/приостановлением его действия.

7.2.9. Применять свой ключ ЭП исключительно в отношениях, определенных областями действия, указанными в связанном с данным ключом ЭП сертификате ключа проверки ЭП.

8. Ответственность сторон

8.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного стороне неисполнением или ненадлежащим исполнением

⁶ Услуга доступна при наличии в ИС функционала, предусмотренного для применения сервиса Службы актуальных статусов сертификатов.

⁷ Услуга доступна при наличии в ИС функционала, предусмотренного для применения сервиса Службы штампов времени.

обязательств, другой стороной. Ни одна из сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая сторона.

8.2. Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если неисполнение либо ненадлежащее исполнение обязательств является следствием встречного неисполнения, либо ненадлежащего встречного исполнения другой стороной своих обязательств в рамках настоящего Регламента.

8.3. УЦ РСХБ не несет ответственности за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях:

- если УЦ РСХБ обоснованно полагался на сведения, указанные в заявлении на регистрацию Субъекта информационного обмена и/или запросе на выдачу сертификата ключа проверки ЭП;

- вследствие компрометации ключа ЭП Субъекта информационного обмена.

8.4. УЦ РСХБ несет ответственность за убытки, возникшие вследствие или в связи с использованием Субъектом информационного обмена сертификата ключа проверки ЭП, выданного УЦ РСХБ только в случае, если указанные убытки возникли вследствие компрометации ключа ЭП Уполномоченного лица Банка.

Субъект информационного обмена понимает и принимает риски, связанные с использованием ЭП и средств ЭП, включая компрометацию ключа ЭП и несанкционированное использование ключа ЭП, при ненадлежащем соблюдении Клиентом мер безопасности.

8.5. Ответственность сторон, не урегулированная положениями настоящего Регламента, регулируется в соответствии с действующим законодательством Российской Федерации.

9. Сроки действия криптографических ключей и сертификатов ключей проверки электронной подписи

9.1. Сроки действия криптографических ключей и сертификатов ключей проверки электронной подписи Уполномоченного лица Банка.

9.1.1. Срок действия ключа ЭП Уполномоченного лица Банка составляет 3 года.

Началом срока действия ключа ЭП Уполномоченного лица Банка считается дата и время начала действия, связанного с данным ключом сертификата ключа проверки ЭП Уполномоченного лица Банка, определяемые по атрибуту сертификата ключа проверки ЭП «Действителен с».

Срок действия сертификата ключа проверки ЭП, соответствующего ключу ЭП Уполномоченного лица Банка, составляет 3 года.

9.1.2. В течение периода от 1 (одного) года до 15 (пятнадцати) месяцев с начала срока действия ключа ЭП Уполномоченного лица Банка отмеченный ключ используется для подписания сертификатов ключей проверки ЭП Субъектов информационного обмена и CRL УЦ РСХБ.

По истечению указанного срока ключ ЭП Уполномоченного лица Банка подвергается процедуре плановой смены, после которой используется для подписания CRL, выдаваемых УЦ РСХБ в течение всего оставшегося срока действия.

9.1.3. Плановая смена криптографических ключей Уполномоченного лица Банка в связи с истечением установленного срока их действия осуществляется в порядке, предусмотренном настоящим Регламентом.

9.2. Сроки действия ключей и сертификатов ключей проверки электронной подписи Субъектов информационного обмена.

9.2.1. Максимальный срок действия ключа ЭП Субъекта информационного обмена составляет 15 (пятнадцать) месяцев.

Началом срока действия ключа ЭП Субъекта информационного обмена считается дата и время начала действия, связанного с этим ключом ЭП сертификата ключа проверки ЭП, выданного УЦ РСХБ, определяемые по атрибуту сертификата «Действителен с».

Срок действия сертификата ключа проверки ЭП, соответствующего ключу ЭП Субъекта информационного обмена, определяется по атрибутам сертификата «Действителен с».

9.2.2. Плановая смена ключей проверки ЭП Субъектов информационного обмена производится не реже 1 (одного) раза в год в порядке, предусмотренном настоящим Регламентом для создания и получения ключей проверки ЭП и сертификатов ключа проверки ЭП.

9.2.3. Сертификат ключа проверки ЭП прекращает свое действие:

- в связи с истечением установленного срока его действия;
- в связи с истечением срока, на который действие сертификата ключа проверки ЭП было приостановлено, если в период отмененного срока действие сертификата не было возобновлено в установленном настоящим Регламентом порядке;
- на основании заявления владельца сертификата ключа проверки ЭП, подаваемого в порядке, предусмотренном настоящим Регламентом;
- в случае прекращения деятельности УЦ РСХБ без перехода его функций другим лицам;
- в случае если УЦ РСХБ стало достоверно известно о прекращении действия документа, на основании которого выдан сертификат, в том числе прекращении действия Комплекта документов;
- в иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ РСХБ и владельцем сертификата ключа проверки ЭП.

9.2.4. Срок действия временных криптографических ключей (временного ключа ЭП и временного ключа проверки ЭП) составляет 45 (сорок пять) календарных дней.

Началом срока действия временного ключа ЭП Субъекта информационного обмена считается дата и время начала действия, связанного с указанным ключом ЭП временного сертификата ключа проверки ЭП, определяемые по атрибуту сертификата ключа проверки ЭП «Действителен с».

Срок действия временного сертификата ключа проверки ЭП, соответствующего временному ключу ЭП Субъекта информационного обмена, составляет 45 (сорок пять) календарных дней.

9.3. Хранение сертификатов ключа проверки электронной подписи в УЦ РСХБ.

Хранение сертификата ключа проверки ЭП в реестре УЦ РСХБ осуществляется в течение всего срока деятельности УЦ РСХБ, если более короткий срок не установлен нормативными правовыми актами.

10. Регистрация Субъекта информационного обмена в реестре УЦ РСХБ

10.1. Регистрация Субъекта информационного обмена в ручном режиме.

10.1.1. Подача Субъектом информационного обмена заявления на регистрацию Субъекта информационного обмена⁸ (далее – Заявление) ОР осуществляется лично физическим лицом, проходящим процедуру регистрации, и исключительно в течение рабочего дня ОР.

⁸ Приложение 7 к настоящему Регламенту.

10.1.2. При приеме Заявления ОР идентифицирует личность Субъекта информационного обмена с использованием документа, удостоверяющего личность⁹.

В процессе приема Заявления ОР вправе запросить, а Субъект информационного обмена должен представить следующие документы:

– документы, подтверждающие сведения, необходимые для идентификации Субъекта информационного обмена, а именно: фамилия, имя, отчество, наименование и номер документа, удостоверяющего личность, дата и место его выдачи, место регистрации¹⁰, СНИЛС;

– удостоверенные надлежащим образом документы, содержащие сведения об организационно-правовой форме организации и наименовании подразделения Субъекта информационного обмена¹¹.

Номер мобильного телефона предоставляется Субъектом информационного обмена для реализации функции обратной связи (ответного звонка) в случае компрометации ключа ЭП или подозрения на компрометацию ключа ЭП.

10.1.3. В процессе идентификации заявителя ОР в день подачи Заявления принимает решение о приеме или отказе в приеме указанного Заявления, и учиняет соответствующую отметку на экземпляре Заявления, который возвращает Субъекту информационного обмена.

ОР может отказать в приеме Заявления в случае отсутствия у заявителя документов, необходимых для его идентификации в соответствии с пунктом 10.1.2 настоящего Регламента, а также в случае ненадлежащего оформления заявления на регистрацию СИО.

10.1.4. Оператором Центра регистрации выполняются регистрационные действия по занесению регистрационной информации в реестры УЦ РСХБ.

10.1.5. Процедура обработки Заявления осуществляется в течение не более 3 (трех) рабочих дней, следующих за рабочим днем, в течение которого Заявление было принято ОР.

10.2. Регистрация Субъекта информационного обмена средствами ИС.

10.2.1. Под регистрацией Субъектов информационного обмена средствами ИС в УЦ РСХБ понимается внесение в реестры УЦ РСХБ регистрационной информации о Субъекте информационного обмена на основании электронного документа, сформированного с использованием ИС, с последующим предоставлением Субъектом информационного обмена Заявления на бумажном носителе.

10.2.2. Подача Субъектом информационного обмена письменного Заявления осуществляется в соответствии с п.10.1.1-10.1.3 настоящего Регламента.

11. Создание сертификата ключа проверки электронной подписи

11.1. Создание сертификата ключа проверки электронной подписи с использованием временного комплекта ключей ЭП.

11.1.1. В процессе регистрации Субъекта информационного обмена Оператор Центра регистрации:

- изготавливает и записывает на ключевой носитель временную ключевую пару в форме ключевого контейнера;

- изготавливает временный сертификат ключа проверки ЭП и обеспечивает включение указанного сертификата в Реестр созданных сертификатов ключей проверки ЭП УЦ РСХБ;

- записывает сформированный временный сертификат ключа проверки ЭП на ключевой носитель;

⁹ Паспорт или иной документ, удостоверяющий личность в соответствии с законодательством Российской Федерации.

¹⁰ Оригинал или нотариально заверенная копия паспорта или иного документа, удостоверяющего личность в соответствии с законодательством Российской Федерации.

¹¹ В случае наличия данных сведений в заявлении на регистрацию Субъекта информационного обмена.

- ключевой носитель помещает в упаковку, для обеспечения возможности контроля целостности упаковки, оклеивает голографической наклейкой;
- передает упакованный ключевой носитель ОР.

11.1.2. Передача Субъекту информационного обмена ключевого носителя с временным комплектом ключей ЭП осуществляется исключительно в течение рабочего дня ОР лично Субъекту информационного обмена ОР, после сообщения ОР о возможности передачи ключевого носителя, и в сроки, установленные Комплектом документов, предусматривающим срок передачи материалов Клиенту не позднее 7 (семи) рабочих дней, следующих за рабочим днем, в течение которого Заявление было принято ОР.

11.1.3. Факт передачи ключевого носителя, а также целостность его упаковки подтверждается собственноручной подписью Субъекта информационного обмена в расписке о получении ключевого носителя с временными ключами ЭП и соответствующим им временным сертификатом ключа проверки ЭП по форме Приложения 8 к настоящему Регламенту.

11.1.4. Создание сертификата ключа проверки ЭП для зарегистрированного Субъекта информационного обмена осуществляется УЦ РСХБ на основании запроса на выдачу сертификата ключа проверки ЭП в электронной форме и его копии на бумажном носителе.

11.1.5. Запрос на выдачу сертификата ключа проверки ЭП в электронной форме формируется с использованием сертификата ключа проверки ЭП, ранее выданного УЦ РСХБ для данного Субъекта¹², и криптографических ключей, связанных с указанным сертификатом, и подается в УЦ РСХБ зарегистрированным Субъектом информационного обмена со своего рабочего места посредством программного обеспечения, предоставляемого Банком.

Запрос на выдачу сертификата ключа проверки ЭП в электронной форме представляет собой данные в формате PKCS#10, содержащиеся в электронном документе, формат которого зависит от программного обеспечения, используемого при его формировании.

Значение поля Subject, содержащегося в запросе на выдачу сертификата ключа проверки ЭП, должно быть идентично значению этого поля в сертификате ключа проверки ЭП, соответствующего ключу ЭП Субъекта информационного обмена, которым сформирована ЭП под подаваемым запросом на выдачу сертификата ключа проверки ЭП Субъекта информационного обмена.

11.1.6. В процессе формирования и передачи в УЦ РСХБ запроса на выдачу сертификата ключа проверки ЭП в электронной форме, Субъект информационного обмена изготавливает две копии указанного запроса на бумажном носителе в соответствии с примером, приведенным в Приложении 9 к настоящему Регламенту, и подписывает их собственноручной подписью. Данная подпись заверяется руководителем организации, лицом, исполняющим его обязанности, или иным лицом, имеющим право на распоряжение финансовыми средствами Клиента.

11.1.7. Копии запроса на выдачу сертификата ключа проверки ЭП на бумажном носителе должны быть переданы ОР посредством почтовой/курьерской связи или лично Субъектом информационного обмена ОР в течение его рабочего дня.

11.1.8. Предоставление копий запроса на выдачу сертификата ключа проверки ЭП на бумажном носителе ОР посредством почтовой/курьерской связи или лично Субъектом информационного обмена ОР является фактом подтверждения владения ключом ЭП Субъектом информационного обмена, доказательством которого также является криптографическая демонстрация эквивалентности обладания ключом электронной подписи.

¹² В случае, когда запрос на выдачу сертификата ключа проверки ЭП формируется Субъектом информационного обмена впервые, применяется ранее выданный временный сертификат ключа проверки ЭП. В случае, когда запрос на выдачу сертификата ключа проверки ЭП формируется при плановой смене сертификата ключа проверки ЭП, применяется сертификат ключа проверки ЭП, в связи с окончанием срока действия которого осуществляется плановая смена.

11.1.9. ОР принимает решение о приеме или отказе в приеме запроса на выдачу сертификата ключа проверки ЭП и учиняет соответствующую отметку на копии запроса на выдачу сертификата ключа проверки ЭП, которую возвращает Субъекту информационного обмена.

11.1.10. Работники УЦ РСХБ принимают к исполнению поступивший от зарегистрированного Субъекта информационного обмена запрос на выдачу сертификата ключа проверки ЭП и осуществляют сверку запроса на выдачу сертификата ключа проверки ЭП в электронной форме с его копией на бумажном носителе, а также проверяют соответствие сведений, в том числе полномочий Субъекта информационного обмена, содержащихся в запросе на выдачу сертификата ключа проверки ЭП, Комплекту документов, устанавливающему отношения, между Клиентом и Банком.

11.1.11. В случае если запрос на выдачу сертификата ключа проверки ЭП не прошел проверку, предусмотренную пунктом 11.1.10 настоящего Регламента, Субъекту информационного обмена может быть отказано в выдаче сертификата ключа проверки ЭП. В этом случае ОР направляет Субъекту информационного обмена официальное уведомление с указанием причины отказа по электронному адресу, определенному для данных целей Комплектом документов, не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было принято решение об отказе.

При положительном результате всех проверок УЦ РСХБ создаёт сертификат ключа проверки ЭП на основе соответствующего запроса, поступившего в электронной форме, и его копии на бумажном носителе.

11.1.12. Принятый УЦ РСХБ запрос на выдачу сертификата ключа проверки ЭП должен быть рассмотрен, и, в случае положительного результата проверок, сертификат ключа проверки ЭП должен быть изготовлен и включен в реестры УЦ РСХБ не позднее 3 рабочих дней, следующих за рабочим днем, в течение которого бумажная копия запроса на выдачу сертификата ключа проверки ЭП была принята ОР.

11.1.13. Сертификат ключа проверки ЭП на бумажном носителе выдаётся владельцу сертификата ключа проверки ЭП на основании Заявления о предоставлении сертификата ключа проверки электронной подписи на бумажном носителе, выполненного по форме Приложения 15 к настоящему Регламенту. ОР передает сертификат ключа проверки электронной подписи его владельцу не позднее 10 (десяти) рабочих дней, следующих за рабочим днем, когда соответствующее Заявление поступило в Банк.

Сертификат ключа проверки ЭП считается признанным Субъектом информационного обмена в случае начала использования Субъектом информационного обмена этого сертификата ключа проверки ЭП или передачи заверенного Субъектом информационного обмена своей рукописной подписью сертификата ключа проверки ЭП на бумажном носителе ОР.

11.2. Создание сертификата ключа проверки электронной подписи с использованием функционала ИС.

11.2.1. Запрос на выдачу сертификата ключа проверки ЭП в электронной форме формируется и подается в УЦ РСХБ зарегистрированным Субъектом информационного обмена на своем рабочем месте с использованием функционала ИС.

11.2.2. Обработка запроса и создание сертификата ключа проверки ЭП происходит в соответствии с пунктами 11.1.4-11.1.13.

12. Аннулирование сертификата ключа проверки электронной подписи

12.1. Аннулирование сертификата ключа проверки ЭП, выданного УЦ РСХБ, осуществляется на основании Запроса на аннулирование сертификата ключа проверки электронной подписи Субъекта информационного обмена (далее – Запрос на аннулирование), подаваемого:

– в виде документа на бумажном носителе в двух экземплярах, выполненного по форме Приложения 10 к настоящему Регламенту;

– владельцем сертификата ключа проверки ЭП в устной форме непосредственно в УЦ РСХБ по его контактными телефонам, приведенным в Комплексе документов.

12.2. Запрос на аннулирование на бумажном носителе.

12.2.1. ОР при приеме Запроса на аннулирование на бумажном носителе выполняет идентификацию заявителя, устанавливая личность с использованием документа, удостоверяющего личность¹³.

12.2.2. ОР в процессе идентификации заявителя в день подачи Запроса на аннулирование принимает решение о приеме или отказе в приеме указанного запроса и унияет соответствующую отметку на экземпляре Запроса на аннулирование, который возвращает заявителю.

12.2.3. ОР может отказать в приеме Запроса на аннулирование в случае отсутствия у заявителя документа, удостоверяющего личность, а также в случае ненадлежащего оформления Запроса на аннулирование.

12.2.4. Работники УЦ РСХБ принимают к исполнению Запрос на аннулирование и осуществляют сверку данных Субъекта информационного обмена и сертификата ключа проверки ЭП, Запрос на аннулирование которого подан, содержащихся в указанном запросе, с данными Субъекта информационного обмена и сертификата ключа проверки ЭП, хранящимися в реестрах УЦ РСХБ.

В случае принятия положительного решения об аннулировании сертификата ключа проверки ЭП, работники УЦ РСХБ включают сведения об аннулированном сертификате ключа проверки ЭП в CRL, издаваемый УЦ РСХБ не позднее 1 (одного) рабочего дня, следующего за рабочим днем, в течение которого Запрос на аннулирование был принят ОР.

12.2.5. В случае если Запрос на аннулирование не прошел проверку, предусмотренную пунктом 12.2.4 настоящего Регламента, заявителю может быть отказано в аннулировании сертификата ключа проверки ЭП. В этом случае ОР направляет заявителю официальное уведомление с указанием причины отказа по электронному адресу, определенному для данных целей Комплектом документов, не позднее 1 (одного) рабочего дня, следующего за рабочим днем, в течение которого Запрос на аннулирование был принят ОР.

12.2.6. Датой аннулирования сертификата ключа проверки ЭП признается дата публикации CRL, содержащего сведения о сертификате ключа проверки ЭП, Запрос на аннулирование которого был подан заявителем.

12.3. Запрос на аннулирование в устной форме.

12.3.1. Подача Запроса на аннулирование в устной форме возможна только в течение рабочего дня УЦ РСХБ.

Запрос в устной форме производится по контактному телефону УЦ РСХБ. При этом, заявитель должен сообщить уполномоченному работнику УЦ РСХБ следующую информацию:

- идентификационные данные владельца сертификата ключа проверки ЭП;
- номер СНИЛС;
- номер мобильного телефона.

12.3.2. Идентификация заявителя при подаче Запроса на аннулирование в устной форме осуществляется посредством ответного звонка работника УЦ РСХБ по телефонному номеру Субъекта информационного обмена, указанному в Комплексе документов.

¹³ Паспорт или иной документ, удостоверяющий личность в соответствии с законодательством Российской Федерации.

12.3.3. При положительной идентификации заявителя работник УЦ РСХБ приостанавливает действие указанного заявителем сертификата ключа проверки ЭП путем внесения сведений о нем в CRL.

12.3.4. Датой начала приостановления действия сертификата ключа проверки ЭП признается дата публикации CRL, содержащего сертификат ключа проверки ЭП, устный запрос на аннулирование которого был подан.

12.3.5. Аннулирование сертификата ключа проверки ЭП производится на основании письменного запроса на аннулирование, предоставляемого владельцем сертификата ключа проверки ЭП в соответствии с п. 12.2 настоящего Регламента.

13. Приостановление действия сертификата ключа проверки электронной подписи

13.1. Действие сертификата ключа проверки ЭП, созданного УЦ РСХБ, может быть приостановлено на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата ключа проверки ЭП составляет 10 (десять) дней с момента включения сведений о приостанавливаемом сертификате ключа проверки ЭП в CRL, издаваемый УЦ РСХБ.

13.2. Приостановление действия сертификата ключа проверки ЭП Субъекта информационного обмена осуществляется на основании запроса на приостановление действия сертификата ключа проверки ЭП (далее – Запрос на приостановление) в виде документа на бумажном носителе в двух экземплярах, выполненного по форме Приложения 11 к настоящему Регламенту, ОР владельцем сертификата ключа проверки ЭП или Уполномоченным должностным лицом.

13.3. Подача Запроса на приостановление осуществляется лично заявителем ОР и исключительно в течение рабочего дня ОР.

13.4. ОР при приеме Запроса на приостановление выполняет идентификацию заявителя, устанавливая личность с использованием документа, удостоверяющего личность¹⁴.

13.5. ОР в процессе идентификации заявителя в день подачи Запроса на приостановление принимает решение о приеме или отказе в приеме указанного запроса и унияет соответствующую отметку на экземпляре Запроса на приостановление, который возвращает заявителю.

ОР может отказать в приеме Запроса на приостановление в случае отсутствия у заявителя документа, удостоверяющего личность, а также в случае ненадлежащего оформления Запроса на приостановление.

13.6. Работники УЦ РСХБ принимают к исполнению Запрос на приостановление и осуществляют сверку данных Субъекта информационного обмена и сертификата ключа проверки ЭП, Запрос на приостановление которого подан, содержащиеся в указанной копии, с данными Субъекта информационного обмена и сертификата, хранящимися в реестрах УЦ РСХБ, и, в случае их совпадения, принимают решение о приостановлении действия сертификата ключа проверки ЭП путем включения сведений о приостанавливаемом сертификате ключа проверки ЭП в CRL, издаваемый УЦ РСХБ, не позднее 1 (одного) рабочего дня, следующего за рабочим днем, в течение которого указанный запрос был принят ОР.

13.7. В случае если запрос на приостановление действия сертификата ключа проверки ЭП не прошел проверку, предусмотренную пунктом 13.6 настоящего Регламента, заявителю может быть отказано в приостановлении действия сертификата ключа проверки ЭП. В этом случае ОР направляет заявителю официальное уведомление с указанием причины отказа по электронному адресу, определенному для данных целей Комплектом документов, не позднее одного рабочего дня, следующего за рабочим днем, в течение которого запрос был принят ОР.

¹⁴ Паспорт или иной документ, удостоверяющий личность в соответствии с законодательством Российской Федерации.

13.8. Датой начала приостановления действия сертификата ключа проверки ЭП признается дата публикации CRL, содержащего сертификат ключа проверки ЭП, запрос о приостановлении действия которого был подан.

14. Возобновление действия сертификата ключа проверки электронной подписи

14.1. Возобновление действия сертификата ключа проверки ЭП, созданного УЦ РСХБ, возможно только в течение срока, на который ранее было приостановлено действие этого сертификата ключа проверки ЭП.

14.2. Возобновление действия сертификата ключа проверки ЭП Субъекта информационного обмена осуществляется УЦ РСХБ на основании Запроса на возобновление действия сертификата ключа проверки электронной подписи Субъекта информационного обмена (далее – Запрос на возобновление), подаваемого его владельцем в двух экземплярах в виде документа на бумажном носителе, выполненного по форме Приложения 12 к настоящему Регламенту, ОР лично владельцем сертификата ключа проверки ЭП¹⁵.

14.3. Запрос на возобновление на бумажном носителе подписывается собственноручной подписью владельца сертификата ключа проверки ЭП и лично подается ОР в течение рабочего дня ОР.

14.4. ОФРО при приеме Запроса на возобновление выполняет идентификацию личности владельца сертификата ключа проверки ЭП с использованием документа, удостоверяющего личность¹⁶.

14.5. ОФРО в процессе идентификации заявителя в день подачи Запроса на возобновление принимает решение о приеме или отказе в приеме указанного запроса и унияет соответствующую отметку на экземпляре Запроса на возобновление, который возвращает Субъекту информационного обмена.

ОР может отказать в приеме указанного запроса в случае отсутствия у заявителя документа, удостоверяющего личность, отсутствия должным образом оформленной доверенности у доверенного лица заявителя, а также в случае ненадлежащего оформления Запроса на возобновление.

14.6. Работники УЦ РСХБ принимают к исполнению Запрос на возобновление и сверяют данные Субъекта информационного обмена и сертификата ключа проверки ЭП, Запрос на возобновление которого подан, с данными Субъекта информационного обмена и сертификата ключа проверки ЭП, хранящимися в реестрах УЦ РСХБ. В случае если указанные сведения совпадают, а срок приостановления действия сертификата ключа проверки ЭП не истек, принимается решение о возобновлении действия сертификата ключа проверки ЭП путем исключения его из CRL УЦ РСХБ не позднее 1 (одного) рабочего дня, следующего за рабочим днем, в течение которого запрос был подан ОР.

14.7. В случае если Запрос на возобновление не прошел проверку, предусмотренную пунктом 14.6 настоящего Регламента, Субъекту информационного обмена может быть отказано в приостановлении действия сертификата ключа проверки ЭП. В этом случае ОР направляет зарегистрированному Субъекту информационного обмена официальное уведомление с указанием причины отказа по электронному адресу, определенному для данных целей Комплектом документов, не позднее одного рабочего дня, следующего за рабочим днем, в течение которого указанный запрос был принят ОР.

14.8. Датой возобновления действия сертификата ключа проверки ЭП признается дата публикации CRL, не содержащего сертификат ключа проверки ЭП, запрос о возобновлении действия которого был подан его владельцем.

¹⁵ Формирование бланка запроса на возобновление сертификата ключа проверки ЭП Субъекта информационного обмена может осуществляться при наличии данного функционала в ИС.

¹⁶ Паспорт или иной документ, удостоверяющий личность в соответствии с законодательством Российской Федерации.

15. Смена криптографических ключей Уполномоченного лица Банка

15.1. Плановая смена криптографических ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) Уполномоченного лица Банка выполняется не ранее, чем через 1 (один) год и не позднее, чем через 15 (пятнадцать) месяцев после начала действия ключа ЭП Уполномоченного лица Банка.

15.2. Внеплановая смена ключей Уполномоченного лица Банка выполняется в случае установления факта компрометации (или подозрения на наличие такого факта) ключа ЭП Банка. Сертификат ключа проверки ЭП Уполномоченного лица в этом случае аннулируется. Все сертификаты ключей проверки ЭП, подписанные с использованием скомпрометированного ключа Уполномоченного лица Банка, также считаются аннулированными.

15.3. Уведомление Субъектов информационного обмена о компрометации ключа ЭП Уполномоченного лица Банка осуществляется посредством размещения данной информации на сайте УЦ РСХБ и рассылки соответствующего сообщения при наличии данного функционала в ИС.

15.4. Все подписанные с использованием скомпрометированного ключа ЭП Уполномоченного лица Банка и действовавшие на момент компрометации ключа ЭП Уполномоченного лица сертификаты ключей проверки ЭП, а также сертификаты ключей проверки ЭП, действие которых было приостановлено, подлежат внеплановой смене в порядке, установленном настоящим Регламентом.

16. Смена криптографических ключей Субъекта информационного обмена

16.1. Плановая смена криптографических ключей Субъекта информационного обмена.

16.1.1. Плановая смена криптографических ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) Субъекта информационного обмена выполняется не ранее, чем через 11 (одиннадцать) месяцев и не позднее, чем через 1 (один) год после начала действия ключа ЭП Субъекта информационного обмена.

16.1.2. Процедура плановой смены криптографических ключей Субъекта информационного обмена осуществляется в соответствии с порядком получения сертификата ключа проверки ЭП зарегистрированным Субъектом информационного обмена, установленным в п.п. 11.1.4-11.1.13 настоящего Регламента.

16.2. Внеплановая смена криптографических ключей Субъекта информационного обмена.

16.2.1. Внеплановая смена криптографических ключей Субъекта информационного обмена выполняется в случае установленного факта компрометации криптографических ключей Субъекта информационного обмена (за исключением случая компрометации, связанного с увольнением/отменой или сменой полномочий владельца сертификата ключа проверки ЭП), а также в случае выхода из строя ключевого носителя.

Внеплановая смена криптографических ключей Субъекта информационного обмена не производится в случае изменения наименования Сторон(ы) в связи с изменениями, внесенными в федеральные законы/иные нормативно-правовые акты и вступившими в силу до момента плановой/внеплановой смены сертификатов ключей проверки ЭП. При этом электронный документ, подписанный ЭП до изменения наименования Сторон(ы), ключ проверки которой содержится в сертификате ключа проверки ЭП, выданном УЦ РСХБ в соответствии с порядком, действующим на момент изготовления сертификата ключа проверки ЭП, действует в течение срока действия указанного сертификата и признается Сторонами после изменения наименования Сторон(ы).

16.2.2. Процедура внеплановой смены криптографических ключей Субъекта информационного обмена осуществляется на основании запроса на аннулирование

сертификата ключа проверки ЭП, поступившего в УЦ РСХБ по причине компрометации соответствующего ключа ЭП.

16.2.2.1. Для Субъекта информационного обмена, использующего временный комплект ключей ЭП, процедура внеплановой смены криптографических ключей осуществляется после процедуры аннулирования сертификата ключа проверки ЭП в установленном настоящим Регламентом порядке. Оператор ЦР на основании Заявления на повторное изготовление временного сертификата ключа проверки электронной подписи, поданного зарегистрированным Субъектом информационного обмена по форме Приложения 14 к настоящему Регламенту, формирует на ключевой носитель временную ключевую пару и соответствующий ей временный сертификат ключа проверки ЭП.

Передача ключевого носителя Субъекту информационного обмена осуществляется путем обмена на ключевой носитель, который ранее использовался Субъектом информационного обмена¹⁷, и в соответствии с п.п. 11.1.2-11.1.3 настоящего Регламента.

Создание сертификата ключа проверки ЭП Субъектом информационного обмена осуществляется согласно п.п. 11.1.4-11.1.13 настоящего Регламента.

16.2.2.2. Для Субъектов информационного обмена, не использующих временный комплект ключей ЭП, порядок получения ключевой пары и соответствующий ей сертификат ключа проверки ЭП совпадает с первичным процессом генерации ключей ЭП и соответствующего им сертификата ключа проверки ЭП и осуществляется в соответствии с п. 11.2 настоящего Регламента.

17. Порядок действий владельца сертификата ключа проверки электронной подписи при компрометации его ключа электронной подписи

17.1. В случае подозрения о компрометации ключа ЭП владелец сертификата ключа проверки ЭП самостоятельно принимает решение о факте компрометации принадлежащего ему ключа ЭП.

17.2. В случае компрометации или подозрения о компрометации ключа ЭП Субъект информационного обмена связывается с УЦ РСХБ по телефону и аннулирует действие сертификата ключа проверки ЭП, соответствующего скомпрометированному ключу, в порядке, установленном п. 12.3 настоящего Регламента.

17.3. Запрос на аннулирование на бумажном носителе должен быть предоставлен Субъектом информационного обмена при проведении процедуры внеплановой смены ключа проверки ЭП в порядке, установленном п. 12.2 настоящего Регламента.

18. Предоставление сервисов Службы актуальных статусов сертификатов и Службы штампов времени

18.1. УЦ РСХБ оказывает услуги по предоставлению актуальной информации о статусе сертификатов ключей проверки ЭП посредством сервиса Службы актуальных статусов сертификатов¹⁸. Служба актуальных статусов сертификатов по запросам Клиентов УЦ формирует и предоставляет этим Клиентам OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа проверки ЭП. OCSP-ответы представляются в форме электронного документа, подписанного ЭП с использованием сертификата ключа проверки ЭП Службы актуальных статусов сертификатов УЦ РСХБ. OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- выполнены условия признания ЭП в OCSP-ответе;
- ЭП в OCSP-ответе сформирована с учетом ограничения, содержащегося в сертификате ключа проверки ЭП Службы актуальных статусов сертификатов, а именно:

¹⁷ В случае утраты ранее использовавшегося ключевого носителя, передача нового осуществляется в соответствии с условиями, определенными в Комплексе документов.

¹⁸ Услуга доступна при наличии в ИС соответствующего функционала.

сертификат ключа проверки ЭП Службы актуальных статусов сертификатов в расширении Extended Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.9-«Подпись ответа службы OCSP».

Адреса обращения к Службе актуальных статусов сертификатов УЦ РСХБ – <http://ca1.rshb.ru/ocsp2012/ocsp.srf>, <http://ca2.rshb.ru/ocsp2012/ocsp.srf>.

18.2. УЦ РСХБ оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени¹⁹. Штамп времени, относящийся к подписанному ЭП электронному документу, признается действительным при одновременном выполнении следующих условий:

- выполнены условия признания ЭП в штампе времени;
- ЭП в штампе времени сформирована с учетом ограничения, содержащегося в сертификате ключа проверки ЭП Службы штампов времени, а именно: сертификат ключа проверки ЭП Службы штампов времени в расширении Extended Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.8 – «Установка штампа времени».

Адрес обращения к Службе штампов времени УЦ РСХБ – <http://ca1.rshb.ru/ocsp2012/tsp.srf>, <http://ca2.rshb.ru/ocsp2012/tsp.srf>

19. Хранение материалов УЦ РСХБ

19.1. Документированная информация УЦ РСХБ и сроки ее хранения:

№ п/п	Вид информации	Срок ее хранения
1.	Аннулированные сертификаты ключей проверки ЭП Уполномоченного лица Банка	5 лет с момента аннулирования
2.	Аннулированные сертификаты ключей проверки ЭП Субъектов информационного обмена	5 лет с момента аннулирования
3.	Заявления на регистрацию Субъектов информационного обмена	5 лет с момента поступления заявления Оператору Центра регистрации
4.	Запросы на выдачу сертификата ключей проверки ЭП	10 лет с момента аннулирования/окончания срока действия соответствующего сертификата ключа проверки ЭП
5.	Запросы на аннулирование сертификатов ключей проверки ЭП	10 лет с момента аннулирования соответствующего сертификата ключа проверки ЭП
6.	Запросы на приостановление действия сертификатов ключей проверки ЭП	10 лет с момента аннулирования/окончания срока действия соответствующего сертификата ключа проверки ЭП
7.	Запросы на возобновление действия сертификатов ключей проверки ЭП	10 лет с момента аннулирования/окончания срока действия соответствующего сертификата ключа проверки ЭП»

19.2. Документы УЦ РСХБ на бумажных носителях, в том числе и выданные УЦ РСХБ сертификаты ключей проверки ЭП в виде документов на бумажном носителе, хранятся в порядке и в течение сроков, установленных законодательством об архивном деле Российской Федерации.

19.3. Вся документированная информация УЦ РСХБ, подлежащая архивному хранению, если это не оговорено особо, представляет собой документы временного хранения.

¹⁹ Услуга доступна при наличии в ИС функционала, предусмотренного для применения сервиса Службы штампов времени.

19.4. Документы, срок архивного хранения которых закончился, подлежат уничтожению в порядке, установленном законодательством Российской Федерации об архивном деле и внутренними документами Банка.

20. Порядок актуализации

20.1. Департамент информационной безопасности несет ответственность за пересмотр настоящего Регламента, за рассмотрение предложений работников Банка по его изменению, актуализации.

20.2. Пересмотр настоящего Регламента осуществляется на периодической и внеплановой основе.

20.3. Периодический пересмотр Регламента должен осуществляться не реже одного раза в два года.

20.4. Внеплановый пересмотр Регламента производится в случае изменения законодательных актов Российской Федерации, иных нормативных актов уполномоченных органов, внутренних документов Банка.