



Приложение к Распоряжению
от 18.06.2025 г. № 2423

РЕГЛАМЕНТ
Удостоверяющего центра АО «АЛЬФА-БАНК»,
подчиненного подсистеме Удостоверяющего центра
платформы Цифрового рубля Банка России

Версия 2

Москва 2025

ИСТОРИЯ ВЕРСИЙ	
Версия №	Дата и № Приказа/Распоряжения
1	12.12.2024 № 4833
2	18.06.2025 № 2423

Оглавление

1. Термины и определения	4
2. ОБЩИЕ ПОЛОЖЕНИЯ	7
2.1. Предмет Регламента.....	7
2.2. Сведения ПУЦ.....	7
2.3. Порядок информирования о предоставлении услуг ПУЦ	7
2.4. Условия оказания услуг ПУЦ.....	8
2.5. Внесение изменений в Регламент ПУЦ, прекращение действия Регламента	8
3. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ ПУЦ ФУНКЦИЙ.....	9
4. ПРАВА И ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ СТОРОН	10
5. ПРАВИЛА ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	13
5.1. Регистрация Пользователя ПлЦР.....	13
5.2. Изготовление и получение Сертификата	13
5.3. Аннулирование (отзыв) Сертификата	14
5.4. Подтверждение подлинности ЭП в электронных документах	15
6. УПРАВЛЕНИЕ СЕРТИФИКАТАМИ В УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ	16
6.1. Порядок смены криптографических ключей ПУЦ.....	16
6.2. Порядок смены криптографических ключей Пользователя ПлЦР.....	17
6.3. Сроки действия ключей ЭП ПУЦ и Пользователя ПлЦР	17
6.4. Хранение информации в ПУЦ.....	17
6.5. Структура Сертификата и САС	18
7. КОНФИДЕНЦИАЛЬНОСТЬ	18
7.1. Типы конфиденциальной информации	18
7.2. Типы информации, не являющейся конфиденциальной	18
8. РАЗРЕШЕНИЕ СПОРОВ	18
Приложение № 1	20
Приложение №2	22
Приложение №3	24
Приложение №4	25
Приложение № 5	27

1. Термины и определения

Банк – АО «АЛЬФА-БАНК».

Владелец сертификата ключа проверки электронной подписи (Владелец сертификата) – лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон № 63-ФЗ) порядке выдан Сертификат.

Заявитель – лицо, обращающееся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в ПУЦ за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

Информационная система (ИС) – автоматизированная и/или информационная система Банка, с использованием которой происходит осуществление защищенного электронного документооборота и обмен подписанными ЭП электронными документами между Пользователем ПлЦР и Банком.

Клиенты – физические лица, юридические лица (за исключением кредитных организаций), включая индивидуальных предпринимателей или физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, использующие ЭП для выполнения операций с Цифровым рублем (ЦР).

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ ЭП – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ ЭП ПУЦ – ключ ЭП, соответствующий ключ проверки ЭП которого содержится в Сертификате ПУЦ. Используется ПУЦ для подписания ПУЦ Сертификатов и САС, выдаваемых и публикуемых ПУЦ.

Ключевая пара (криптографические ключи) – ключ ЭП и соответствующий ему ключ проверки ЭП.

Ключевой носитель – мобильное устройство, предназначенное для размещения криптографических ключей Пользователя ПлЦР. Хранение криптографических ключей Клиента, предназначенных для подписания (проверки подписи) и (или) шифрования (расшифрования) на прикладном уровне электронных сообщений в ИС, должно осуществляться на устройстве Клиента в соответствии с требованиями эксплуатационной документации к используемому СКЗИ.

Компрометация ключа – нарушение конфиденциальности ключа электронной подписи, связанное с утратой доверия к тому, что используемый ключ электронной подписи недоступен посторонним лицам, или подозрением, что ключ электронной подписи был временно доступен неуполномоченным лицам. К основным событиям, приводящим к компрометации ключей, относятся, включая, но не ограничиваясь, следующие события:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключей ЭП;
- возникновение подозрений на нарушение конфиденциальности, целостности и доступности передаваемой информации;
- нарушение печати на сейфе, в котором хранятся ключевые носители;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (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).

Платформа Цифрового рубля Банка России (Платформа ЦР, ПлЦР) – информационная система, посредством которой взаимодействуют оператор платформы, участники платформы и пользователи платформы в целях совершения операций с цифровыми рублями. Оператором Платформы ЦР является Банк России, участниками Платформы ЦР являются банки, предоставляющие своим клиентам доступ к Платформе ЦР. Пользователями Платформы ЦР являются физические лица, юридические лица, включая индивидуальных предпринимателей или физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, которым предоставлен доступ к Платформе ЦР.

Представитель Клиента – физическое лицо, уполномоченное клиентом, являющимся юридическим лицом, на регистрацию в Реестрах ПУЦ и получение Сертификата.

Регистрация Пользователя ПлЦР – внесение в Реестры ПУЦ регистрационной информации о Пользователе ПлЦР.

Реестры ПУЦ – набор документов ПУЦ в электронной и/или бумажной форме, включающий следующую информацию:

- реестр запросов на регистрацию Пользователей ПлЦР в ПУЦ;
- реестр зарегистрированных Пользователей ПлЦР;
- реестр запросов на создание и выдачу Сертификатов;
- реестр запросов на аннулирование Сертификатов;
- реестр Сертификатов;
- реестр аннулированных Сертификатов;
- реестр изготовленных САС.

Сертификат ключа проверки электронной подписи (Сертификат) – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. В рамках настоящего Регламента ПУЦ создает и выдает Заявителям только неквалифицированные Сертификаты.

Сертификат ПУЦ – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром Банка России для Банка и подтверждающий принадлежность ключа проверки ЭП Банку.

Список аннулированных сертификатов (САС) – электронный документ с электронной подписью Удостоверяющего Центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были аннулированы (отозваны) или действие которых было прекращено. Момент времени формирования списка отозванных сертификатов определяется по значению поля «Действителен с» списка отозванных сертификатов.

Средства удостоверяющего центра (Средства УЦ) – программное и (или) аппаратное средство, используемое для реализации функций удостоверяющего центра. Средства УЦ используются совместно с сервером точного времени, имеющим сертификат Госстандарта России об утверждении типа измерителей текущих значений времени.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средство криптографической защиты информации (СКЗИ) – шифровальное (криптографическое) средство, реализующее российские криптографические алгоритмы ГОСТ и имеющие действующий сертификат соответствия требованиям ФСБ России.

Пользователь ПлЦР – Клиент или Представитель Клиента, присоединившиеся к настоящему Регламенту, и сведения о которых включены в Реестры ПУЦ.

Удостоверяющий центр АО «АЛЬФА-БАНК», подчиненный подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (ПУЦ) – организация, осуществляющая функции по регистрации Пользователей ПлЦРв ПУЦ, созданию, выдаче и аннулированию Сертификатов Пользователей ПлЦР, а также иные функции, предусмотренные настоящим Регламентом. Для осуществления указанных функций ПУЦ использует комплекс программно-аппаратных средств Банка, предназначенный для осуществления деятельности, предусмотренной Федеральным законом № 63-ФЗ,

Усиленная неквалифицированная ЭП – электронная подпись, соответствующая признакам, установленным ч.3 ст.5 Федерального закона № 63-ФЗ.

Субъекты ПлЦР – Платформа ЦР, Банк и Пользователи ПлЦР, осуществляющие обмен информацией в электронной форме.

Электронный документ – документ, информация в котором представлена в электронной форме.

Электронная подпись (ЭП) – 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.

Public Key Cryptography Standards (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий Центр осуществляет свою работу в соответствии со следующими стандартами PKCS:

- **CMS (PKCS#7)** – стандарт, определяющий формат и синтаксис криптографических сообщений в соответствии с RFC 3852. Банк использует описанный в PKCS#7 тип данных PKCS#7 signed – подписанные данные. Электронный документ, оформленный с соблюдением требований PKCS#7 signed, является электронным документом, содержащим электронную подпись;

- **PKCS#10** – стандарт, определяющий формат и синтаксис запроса на сертификат ключа проверки электронной подписи в соответствии с RFC 2986. Электронный документ, оформленный с соблюдением требований PKCS#10, содержит информацию о сертифицируемом ключе проверки электронной подписи, используемом криптографическом средстве и данные, необходимые для идентификации владельца сертифицируемого ключа проверки электронной подписи.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Предмет Регламента

2.1.1. Настоящий Регламент Удостоверяющего центра АЛЬФА-БАНК, подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (далее – Регламент) определяет условия предоставления услуг ПУЦ, включая права, обязанности и ответственность Пользователей ПлЦР и Банка, порядок регистрации Пользователей ПлЦР в ПУЦ, порядок создания, смены и аннулирования Сертификатов.

2.1.2. ПУЦ осуществляет целевые функции по созданию и выдаче неквалифицированных сертификатов ключей проверки электронной подписи и иные функции удостоверяющего центра в соответствии с требованиями действующей редакции Федерального закона № 63-ФЗ и иными принимаемыми в соответствии с ним правовыми актами.

2.2. Сведения ПУЦ

2.2.1. АКЦИОНЕРНОЕ ОБЩЕСТВО «АЛЬФА-БАНК», зарегистрировано на территории Российской Федерации в городе Москве. Свидетельство о регистрации № 001.937 выдано 24.02.1998 Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1027700067328 от 26.07.2002 г.

2.2.2. Полное наименование: Удостоверяющий центр АЛЬФА-БАНК, подчиненный подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России.

2.2.3. Сокращенное наименование: АО «АЛЬФА-БАНК»

2.2.4. Юридический адрес: 107078, г. Москва, ул. Каланчевская, д. 27

2.2.5. ПУЦ осуществляет свою работу в круглосуточном режиме.

2.2.6. ПУЦ осуществляет свою деятельность на территории Российской Федерации по созданию и выдаче Сертификатов на основании имеющейся у Банка лицензии на осуществление разработки, производства, распространения шифровальных (криптографических) средств, ИС и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, ИС и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, ИС 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 28.07.2016 г. рег. № 15294 Н).

2.3. Порядок информирования о предоставлении услуг ПУЦ

2.3.1. Информирование о предоставлении услуг ПУЦ осуществляется путем публикации Регламента.

2.3.2. Настоящий Регламент размещается:

- в электронной форме в виде файла формата PDF на официальном сайте Банка в сети Интернет по адресу: <https://alfabank.ru/>;
- в форме документа на бумажном носителе в местах обслуживания клиентов.

2.4. Условия оказания услуг ПУЦ

2.4.1. Настоящий Регламент является договором присоединения, утвержденным Банком, в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

2.4.2. Опубликование Регламента, включая распространение его текста в сети «Интернет» на сайте Банка, должно рассматриваться всеми заинтересованными лицами как публичное предложение (оферта) со стороны Банка заключить договор о предоставлении услуг ПУЦ, существенные условия которого содержатся в настоящем Регламенте.

2.4.3. Присоединение Клиента к Регламенту осуществляется путем направления таким Клиентом Заявления на создание и выдачу Сертификата по формам, установленным в Приложениях №1 и 2 к настоящему Регламенту либо путем присоединения Клиента к договору комплексного банковского обслуживания (ДКБО) или иному публичному договору с Банком, предусматривающему получение Клиентом Сертификата в целях использования ЭП для выполнения операций с ЦР (далее - Договор). С момента приема к исполнению указанного Заявления/присоединения к Договору Клиент считается присоединившимся к настоящему Регламенту и становится Стороной Регламента.

2.4.4. Требования настоящего Регламента применяются в течение срока действия Сертификата.

2.4.5. Стороны согласны с тем, что условия настоящего Регламента принимаются Пользователем полностью и безусловно.

2.4.6. Владелец сертификата имеет право в одностороннем порядке прекратить взаимодействие с ПУЦ в рамках Регламента, направив в ПУЦ заявление на прекращение действия выданного ему Сертификата или запрос на аннулирование Сертификата в электронной форме с использованием ИС. При этом договор с ПУЦ считается расторгнутым.

2.5. Внесение изменений в Регламент ПУЦ, прекращение действия Регламента

2.5.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится ПУЦ в одностороннем порядке.

2.5.2. Уведомление о внесении изменений или дополнений в Регламент осуществляется путем размещения соответствующей информации на сайте Банка в сети «Интернет»: <https://alfabank.ru/> за 10 календарных дней до вступления изменений в силу.

2.5.3. Все изменения (дополнения), вносимые ПУЦ в Регламент по собственной инициативе, и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными с даты размещения новой редакции Регламента на сайте Банка по адресу - <https://alfabank.ru/> или в форме документа на бумажном носителе в местах обслуживания клиентов.

2.5.4. Все изменения (дополнения), вносимые ПУЦ в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных законодательных актах.

2.5.5. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

2.5.6. В целях обеспечения своевременного получения информации об изменениях и/или дополнениях в настоящий Регламент, Пользователь ПлЦР обязуется на периодической основе самостоятельно получать сведения об изменениях, которые

планируется внести в настоящий Регламент, с использованием официального сайта Банка в сети Интернет по адресу: <https://alfabank.ru/>.

2.5.7. Банк не несет ответственности за возможные убытки Пользователя ПлЦР, причиненные его неосведомленностью, в случае, если Банк надлежащим образом выполнил свои обязательства по размещению новой редакции Регламента согласно п.2.5.3.

2.5.8. Настоящий Регламент прекращает свое действие при прекращении деятельности ПУЦ. Деятельность ПУЦ может быть прекращена в случаях и порядке, установленных действующим законодательством Российской Федерации. При этом информация, внесенная в Реестры ПУЦ, уничтожается или передается лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность, в соответствии с порядком, установленным действующим законодательством Российской Федерации.

В случае прекращения действия настоящего Регламента соответствующая информация размещается на официальном сайте Банка в сети Интернет по адресу: <https://alfabank.ru/>.

3. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ ПУЦ ФУНКЦИЙ

В перечень реализуемых ПУЦ функций (оказываемых услуг) в соответствии с настоящим Регламентом, входят:

- 3.1. Регистрация Пользователей ПлЦР.
- 3.2. Создание и выдача Сертификатов.
- 3.3. Подтверждение владения Заявителем ключом ЭП, соответствующим ключу проверки ЭП, указанному им для получения Сертификата.
- 3.4. Установление сроков действия Сертификатов.
- 3.5. Аннулирование выданных ПУЦ Сертификатов.
- 3.6. Ведение реестра Сертификатов и аннулированных Сертификатов, в том числе включающий в себя информацию, содержащуюся в выданных ПУЦ Сертификатах, и информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях таких прекращений или аннулирования.
- 3.7. Формирование порядка ведения Реестров ПУЦ и порядок доступа к ним, а также обеспечивает доступ участников электронного взаимодействия к информации, содержащейся в реестре Сертификатов в соответствии с требованиями Федерального закона № 63-ФЗ.
- 3.8. Публикация актуального САС, обеспечение возможности свободного доступа участников электронного взаимодействия к САС.
- 3.9. Проверка уникальности ключей проверки ЭП в реестре Сертификатов.
- 3.10. Проверка действительности ЭП по обращениям Клиентов. Порядок проверки подлинности ЭП состоит в проверке одновременного соблюдения следующих условий:
 - Сертификат выдан ПУЦ;
 - Сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на момент проверки действительности указанного Сертификата, если момент подписания документа не определен;
 - имеется положительный результат проверки принадлежности владельцу Сертификата данной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в данный документ после его

подписания с использованием средств ЭП, имеющих подтверждение соответствия требованиям Федерального закона № 63-ФЗ;

- ЭП используется в отношениях, определенных областями действия, указанными в Сертификате лица, подписывающего электронный документ.

3.11. Предъявление требований по обеспечению информационной безопасности при использовании ключей ЭП и средств ЭП в процессе осуществления юридически значимого электронного документооборота между Клиентом и Банком путем предоставления.

3.12. Осуществление иной деятельности, предусмотренной Федеральным законом № 63-ФЗ.

4. ПРАВА И ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ СТОРОН

ПУЦ обязан:

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

Использовать ключ ЭП Банка исключительно для подписи выдаваемых ПУЦ Сертификатов и публикуемых САС.

Принимать меры по защите ключа ЭП Банка от несанкционированного доступа.

Обеспечивать уникальность серийных номеров создаваемых Сертификатов.

Проверять уникальность значений ключей проверки ЭП в созданных Сертификатах Пользователей ПлЦР.

Информировать Пользователей ПлЦР об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

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

Как это установлено действующим законодательством предоставлять в соответствии с требованиями Федерального закона № 63-ФЗ безвозмездно доступ к информации, содержащейся в реестре Сертификатов, реестре аннулированных Сертификатов.

Отказать Пользователю ПлЦР в создании Сертификатов в случае, если не было подтверждено то, что Пользователь ПлЦР владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному Пользователем ПлЦР для получения Сертификатов.

Отказать Пользователю ПлЦР в создании Сертификата в случае отрицательного результата проверки в реестре Сертификатов уникальности ключа проверки ЭП, указанного Пользователем ПлЦР для получения Сертификата.

Соблюдать сроки аннулирования Сертификатов Пользователей ПлЦР.

Осуществлять регистрацию Пользователей ПлЦР на основании заявлений Пользователей ПлЦР, поданных в ПУЦ на бумажном носителе или в электронном виде посредством ИС, а также запросов на выдачу Сертификатов, в соответствии с положениями, определенными настоящим Регламентом.

Обеспечивать занесение регистрационной информации Пользователей ПлЦР в Реестры ПУЦ и обеспечивать уникальность регистрационной информации, используемой для идентификации владельцев Сертификатов.

Обеспечивать конфиденциальность регистрационной информации Пользователей ПлЦР, за исключением информации, заносимой в Сертификаты, выдаваемые ПУЦ.

Осуществлять создание Сертификатов Пользователей ПлЦР в соответствии с нормами, определенными настоящим Регламентом и действующим законодательством.

Обеспечивать внесение информации о созданном Сертификате Пользователя ПлЦР в реестр Сертификатов не позднее указанной в нем даты начала действия такого сертификата.

Аннулировать Сертификат Пользователя ПлЦР путем внесения записи о его аннулировании в САС с указанием даты, времени внесения и причины аннулирования в течение двенадцати часов с момента, когда ПУЦ стало известно или должно было стать известно о наступлении обстоятельств, указанных в ч.6 и 6.1 ст. 14 Федерального закона № 63-ФЗ.

ПУЦ имеет право:

Отказать в предоставлении услуг по регистрации Пользователя ПлЦР в ПУЦ в случае нарушения указанным Пользователем ПлЦР требований настоящего Регламента, с указанием причин отказа.

Отказать в предоставлении услуг по созданию Сертификата Пользователю ПлЦР в случае нарушения указанным П Пользователем ПлЦР требований настоящего Регламента с указанием причин отказа.

Отказать Пользователю ПлЦР в предоставлении услуг по созданию Сертификата в случае, если использованное для формирования запроса на Сертификат средство ЭП не поддерживается ПУЦ.

Отказать владельцу Сертификата в его аннулировании в случае, если истек установленный срок действия ключа ЭП, соответствующего указанному Сертификату.

Аннулировать Сертификат Пользователя ПлЦР в случае установленного факта компрометации соответствующего ключа ЭП, в том числе и без соответствующего заявления со стороны владельца Сертификата, в случае если ПУЦ стало достоверно известно о прекращении действия документа, на основании которого выдан Сертификат, в случае закрытия последнего счета Пользователя ПлЦР, а также в установленных законодательством Российской Федерации случаях с последующим его уведомлением о факте и причине аннулирования.

Пользователь ПлЦР обязан:

Предоставить сведения и документы, необходимые для создания Сертификата, установленные настоящим Регламентом.

Извещать ПУЦ обо всех изменениях данных, внесенных в сертификат.

При подаче заявления на сертификат указать действующий электронный почтовый адрес Владельца сертификата для получения извещений, уведомлений от ПУЦ, связанных с применением сертификата, его аннулированием.

Обеспечить конфиденциальность ключа ЭП. Хранить в тайне Ключ ЭП Пользователя ПлЦР, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

Не применять Ключ ЭП, если пользователю стало известно, что этот ключ используется или использовался ранее другими лицами.

Применять Ключ ЭП только в соответствии с областями действия, указанными в соответствующем данному ключу ЭП сертификате, если такие области действия установлены.

Немедленно обратиться в ПУЦ с заявлением на аннулирование (отзыв) Сертификата в случае утери, кражи, раскрытия, искажения личного ключа ЭП, а также в случае если пользователю стало известно, что этот ключ используется или использовался ранее другими лицами.

Не использовать Ключ ЭП, связанный с Сертификатом, заявление на аннулирование (отзыв) которого подано в ПУЦ, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата по момент времени официального уведомления пользователя об аннулировании (отзыве) сертификата.

Не использовать личный Ключ ЭП, связанный с Сертификатом, который аннулирован (отозван).

Пользователь ПлЦР имеет право:

Обращаться в ПУЦ по вопросам создания и выпуска Сертификата, а также аннулирования Сертификата, владельцем которого он является, в течение срока действия, соответствующего ключа ЭП.

Получать Сертификат как в форме электронного документа, так и в форме документа на бумажном носителе по запросу.

Получать информацию о статусе сертификата и подтверждение его владением на определенный момент времени.

Получать Сертификат Банка и использовать его для проверки ЭП Банка в Сертификатах, выданных ПУЦ.

Обращаться в соответствии с настоящим Регламентом в ПУЦ для проверки подлинности ЭП в электронных документах, подписанных с использованием Сертификатов, выданных ПУЦ.

Обращаться в соответствии с настоящим Регламентом в ПУЦ для аннулирования Сертификата, в течение срока действия данного Сертификата.

Прекратить взаимодействие с ПУЦ в рамках Регламента, направив в ПУЦ заявление на прекращение действия выданного ему Сертификата.

Ответственность Сторон.

За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту стороны несут ответственность в порядке, предусмотренном действующим законодательством Российской Федерации.

ПУЦ не несет ответственности за неисполнение и (или) ненадлежащее исполнение обязательств, убытки, ущерб, расходы, издержки, имущественные потери Заявителя, возникшее не по вине ПУЦ.

ПУЦ не несет ответственности за убытки, ущерб, расходы, издержки, имущественные потери третьих лиц, если это прямо не установлено действующим законодательством.

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

- если ПУЦ обоснованно полагался на сведения, предоставленные Заявителем;
- вследствие компрометации ключа ЭП Пользователя ПлЦР.

ПУЦ несет ответственность за убытки, возникшие вследствие или в связи с использованием Пользователем ПлЦР Сертификата, выданного ПУЦ только в случае, если указанные убытки возникли вследствие компрометации ключа ЭП Банка.

Пользователь ПлЦР понимает и принимает риски, связанные с использованием ЭП и средств ЭП, в том числе:

- несоблюдение обязанности по обеспечению конфиденциальности Ключа ЭП;
- использование Ключа ЭП после подачи заявления на аннулирование Сертификата или после аннулирования Сертификата;
- несанкционированное использование ключа ЭП;

- ненадлежащее соблюдение Пользователем ПлЦР мер безопасности, указанных в руководстве по обеспечению безопасности использования ключей электронной подписи и средств электронной подписи (приложение №5 к Регламенту).

Пользователь ПлЦР несет ответственность за несоблюдение обязанностей по соблюдению мер безопасности Ключа ЭП, в том числе за использование скомпрометированного Ключа ЭП.

Заявитель несет ответственность за достоверность и полноту документов и сведений, предоставляемых в ПУЦ, неисполнение обязанностей, установленных Федеральным законом № 63-ФЗ, настоящим Регламентом.

Ответственность сторон, не урегулированная настоящим Регламентом, регулируется в соответствии с действующим законодательством Российской Федерации.

5. ПРАВИЛА ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

5.1. Регистрация Пользователя ПлЦР

Инициирование регистрации Пользователя ПлЦР в Реестрах ПУЦ осуществляется таким Пользователем ПлЦР с использованием ИС после его успешной идентификации.

5.2. Изготовление и получение Сертификата

Запрос на выдачу Сертификата в электронной форме автоматически формируется и подается Пользователем ПлЦР в ПУЦ с использованием функционала ИС после успешной идентификации Заявителя.

Идентификация Заявителя может осуществляться одним из следующих способов:

в личном присутствии - по основному документу, удостоверяющему его личность в соответствии с действующим законодательством;

без личного присутствия:

- с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме;

- с использованием неквалифицированной электронной подписи, при создании и проверке которой применяются средства электронной подписи и средства удостоверяющего центра, прошедшие в установленном порядке процедуру соответствия требованиям, установленным в соответствии с частью 5 статьи 8 Федерального закона №63, при наличии действующего сертификата ключа проверки электронной подписи, который выдан тем же удостоверяющим центром и в том же порядке, при условии, что при ранее осуществленном обращении заявителя в этот удостоверяющий центр для создания сертификата ключа проверки электронной подписи и выдачи такого сертификата заявителю в отношении усиленной неквалифицированной электронной подписи идентификация заявителя была проведена удостоверяющим центром одним из способов, указанных выше.

Пользователь ПлЦР с использованием ИС автоматически:

1) формирует на основании запроса на выдачу Сертификата заявление на создание и выдачу Сертификата в электронной форме (далее- Заявление);

2) инициирует с использованием ИС передачу заявления в ПУЦ.

Формы заявлений утверждены Приложениями №1 и 2 к настоящему Регламенту.

ПУЦ принимает к исполнению Заявление создает Сертификат на основе запроса на выдачу Сертификата и Заявления и включает его в Реестры ПУЦ не позднее 3 (трех)

рабочих дней, следующих за рабочим днем, в течение которого Заявление было получено ПУЦ.

В случае если Заявление не прошло положительную проверку ПУЦ отказывает в выдаче Сертификата.

Пользователь ПлЦР может использовать Сертификат, выданный согласно пункту 5.2 Регламента, после подтверждения факта ознакомления с информацией, содержащейся в Сертификате.

Виды электронной подписи, используемой Пользователем ПлЦР для подписания Заявления и подтверждения факта ознакомления с информацией, содержащейся в Сертификате, а также условия ее использования, определяются договором комплексного банковского обслуживания (ДКБО)/договором на обслуживание по системе «Альфа-Бизнес Онлайн» и правилами взаимодействия участников системы «Альфа-Бизнес Онлайн», иным публичным договором с Банком, предусматривающим получение Клиентом Сертификата в целях использования ЭП для выполнения операций с ЦР.

Информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Сертификат на бумажном носителе может быть выдан Владельцу сертификата на основании заявления о предоставлении сертификата ключа проверки электронной подписи, предоставленного в ПУЦ на бумажном носителе. ПУЦ передает Сертификат на бумажном носителе его владельцу не позднее 10 (десяти) рабочих дней с момента поступления соответствующего заявления.

При вручении Сертификата ПУЦ информирует Владельца сертификата об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки путем предоставления ему руководства по обеспечению безопасности использования ключей электронной подписи и средств электронной подписи в составе настоящего Регламента (приложение №5).

5.3. Аннулирование (отзыв) Сертификата

ПУЦ аннулирует Сертификат, в следующих случаях:

не подтверждено, что владелец сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;

установлено, что содержащийся в сертификате уже содержится в ином ранее созданном сертификате;

вступило в силу решение суда, которым установлено, что Сертификат содержит недостоверную информацию;

при компрометации ключа ЭП Банка;

закрытие последнего счета Пользователя ПлЦР.

Сертификат прекращает свое действие в следующих случаях:

на основании заявления Владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

в связи с истечением установленного срока его действия;

в случае прекращения деятельности ПУЦ без перехода его функций другим лицам;

в иных случаях, установленных Федеральным законом № 63-ФЗ, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или настоящим Регламентом.

Прекращением действия Сертификата по истечению срока его действия, признается дата и время, указанные в соответствующем поле. Информация о Сертификате, действие которого прекращено по указанному обстоятельству, не вносится ПУЦ в САС.

В случае компрометации ключа ЭП Банка временем аннулирования (отзыва) сертификата Пользователя признается время компрометации ключа ЭП Банка, фиксирующееся в реестре ПУЦ.

Аннулирование Сертификата, выданного ПУЦ, осуществляется на основании:

1) Заявления на аннулирование Сертификата на бумажном носителе, подаваемого Пользователем ПлЦР в ПУЦ при личном присутствии в двух экземплярах, выполненного по форме Приложения 3 к настоящему Регламенту.

ПУЦ при приеме от Пользователя ПлЦР Заявления на аннулирование Сертификата на бумажном носителе выполняет идентификацию Пользователя ПлЦР при его личном присутствии, устанавливая личность с использованием документа, удостоверяющего личность.

ПУЦ в процессе идентификации Пользователя ПлЦР в день подачи Заявления на аннулирование Сертификата принимает решение о приеме или отказе в приеме указанного заявления.

ПУЦ может отказать в приеме Заявления на аннулирование Сертификата в случае отсутствия у Пользователя ПлЦР документа, удостоверяющего личность, а также в случае ненадлежащего оформления Заявления на аннулирование Сертификата.

2) Запроса на аннулирование Сертификата, подаваемого в электронной форме с использованием ИС.

Пользователь ПлЦР инициирует аннулирование Сертификата с использованием ИС.

Виды электронной подписи, используемой Пользователем ПлЦР для подписания Запроса на аннулирование Сертификата, подаваемого в электронной форме с использованием ИС, а также условия ее использования, определяются договором комплексного банковского обслуживания (ДКБО)/договором на обслуживание по системе «Альфа-Бизнес Онлайн» и правилами взаимодействия участников системы «Альфа-Бизнес Онлайн», иным публичным договором с Банком, предусматривающим получение Клиентом Сертификата в целях использования ЭП для выполнения операций с ЦР.

Информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

ИС направляет запрос на аннулирование Сертификата в ПУЦ.

ПУЦ при положительном рассмотрении запроса на аннулирование Сертификата аннулирует Сертификат Пользователя ПлЦР.

В случае аннулирования Сертификата по заявлению/запросу Пользователя ПлЦР ПУЦ должен официально уведомить Пользователя ПлЦР об аннулировании Сертификата не позднее одного рабочего дня с момента подачи заявления в ПУЦ/создания запроса в ИС.

Официальным уведомлением о факте отзыва Сертификата является опубликование первого (наиболее раннего) САС, содержащего сведения об аннулированном Сертификате, и изданного не ранее времени наступления произошедшего случая. Датой аннулирования Сертификата признается дата публикации САС, содержащего сведения о Сертификате, запрос на аннулирование которого был подан Пользователем ПлЦР.

Информация о размещении САС заносится в изданные ПУЦ сертификаты в расширение CRL Distribution Point Сертификата.

5.4. Подтверждение подлинности ЭП в электронных документах

5.4.1. Подтверждение подлинности ЭП в электронных документах осуществляется на основании заявления на проверку подлинности электронной подписи в электронном документе, форма которого утверждена Приложением № 4 к настоящему Регламенту.

5.4.2. Заявление может быть подано как в форме бумажного документа, подписанного собственноручной подписью Заявителя либо в форме электронного документа.

5.4.3. Срок проведения работ составляет не позднее 30 (тридцати) рабочих дней с момента поступления заявления в ПУЦ.

5.4.4. В ходе проведения работ ПУЦ может быть запрошена дополнительная информация.

5.4.5. Процедура подтверждения действительности ЭП осуществляется с использованием специализированного программного обеспечения, входящего в состав средства ПУЦ, комиссией, состоящей из уполномоченных лиц ПУЦ (не менее 3х человек). По согласованию сторон в комиссию могут входить представители заявителя или уполномоченные сотрудники правоохранительных органов

5.4.6. В ходе процедуры подтверждения действительности ЭП комиссией осуществляется проверка всех сертификатов, на основании которых были сформированы ЭП на документах, определение даты формирования каждой ЭП в документах, проверку каждого сертификата в цепочке до корневого сертификата ПУЦ, проверку действительности всех сертификатов на момент проверки и отсутствие их в САС.

5.4.7. Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение/протокол проверки ЭП в электронном документе, в общем случае включающий в себя:

- основание для проведения проверки;
- данные, представленные комиссии для проведения проверки;
- время и место проведения проверки;
- содержание и результат проверки каждого сертификата в цепочке до корневого сертификата ПУЦ;
- обоснование результатов проверки.

5.4.8. Заключение/протокол проверки ЭП в электронном документе составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью. Один экземпляр - предоставляется Пользователю ПлЦР, второй экземпляр - хранится в ПУЦ.

6. УПРАВЛЕНИЕ СЕРТИФИКАТАМИ В УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

6.1. Порядок смены криптографических ключей ПУЦ

Смена криптографических ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) ПУЦ осуществляется в связи с истечением срока их действия (далее – плановая смена ключа ЭП).

Плановая смена криптографических ключей Банка выполняется в период действия ключа ЭП ПУЦ.

Внеплановая смена криптографических ключей ПУЦ выполняется в случае установления факта компрометации (или подозрения на наличие такого факта) ключа ЭП ПУЦ. Сертификат ПУЦ в таком случае аннулируется. Все Сертификаты, подписанные с использованием скомпрометированного ключа ЭП ПУЦ, также считаются аннулированными.

Уведомление Пользователя ПлЦР о компрометации ключа ЭП ПУЦ осуществляется посредством размещения данной информации на сайте Банка в сети Интернет по адресу: <https://alfabank.ru/>.

Все подписанные с использованием скомпрометированного ключа ЭП ПУЦ и действовавшие на момент компрометации ключа ЭП ПУЦ Сертификаты Пользователя ПлЦР подлежат внеплановой смене в порядке, установленном настоящим Регламентом.

Процедура плановой и внеплановой смены криптографических ключей ПУЦ осуществляется в порядке, установленном Регламентом взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платформы Цифрового рубля.

6.2. Порядок смены криптографических ключей Пользователя ПлЦР

Смена криптографических ключей Пользователя ПлЦР выполняется в случае истечения срока действия Сертификата Пользователя ПлЦР, установленного факта компрометации криптографических ключей Пользователя ПлЦР, в случае выхода из строя ключевого носителя, а также в случае изменения данных Пользователя ПлЦР, содержащихся в учетной записи Реестра ПУЦ и в Сертификате Пользователя ПлЦР, а также в иных случаях, предусмотренных настоящим Регламентом.

Смена Сертификата Пользователя ПлЦР осуществляется согласно разделу 5.2 настоящего Регламента.

В случае установленного факта компрометации криптографических ключей Пользователя ПлЦР, в случае выхода из строя ключевого носителя, а также в случае изменения данных Пользователя ПлЦР, содержащихся в учетной записи Реестра ПУЦ и в Сертификате Пользователя ПлЦР необходимо предварительно аннулировать Сертификат согласно разделу 5.3 настоящего Регламента.

6.3. Сроки действия ключей ЭП ПУЦ и Пользователя ПлЦР

Сроки действия ключей ЭП ПУЦ и Пользователя ПлЦР устанавливаются в соответствии с Правилами заполнения полей сертификатов Платформы ЦР (ЦБРФ.62.0.39725.ПЕ.Э).

Начало периода действия ключа ЭП Банка исчисляется с даты и времени его генерации.

Начало периода действия ключа ЭП Пользователя ПлЦР исчисляется с даты и времени начала действия соответствующего сертификата.

6.4. Хранение информации в ПУЦ

ПУЦ в течение всего срока своей деятельности, если другие сроки не установлены законодательством Российской Федерации, хранит информацию, внесенную в реестры ПУЦ.

Документы на бумажных носителях, в том числе и выданные ПУЦ Сертификаты в виде документов на бумажном носителе, хранятся в порядке и в течение сроков, установленных законодательством Российской Федерации об архивном деле.

Документы, срок архивного хранения которых закончился, подлежат уничтожению в порядке, установленном законодательством Российской Федерации об архивном деле.

Хранение информации осуществляется в форме, позволяющей проверить ее целостность и достоверность.

6.5. Структура Сертификата и САС

ПУЦ формирует сертификаты и САС в электронной форме в соответствии с рекомендациями IETF RFC 5280 (2008) «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».

Структура и состав Сертификатов ПУЦ и Пользователя ПлЦР определяются в соответствии с Правилами заполнения полей сертификатов Платформы ЦР (ЦБРФ.62.0.39725.ПЕ.Э).

7. КОНФИДЕНЦИАЛЬНОСТЬ

7.1. Типы конфиденциальной информации

Ключ ЭП, соответствующий Сертификату Пользователя ПлЦР, является конфиденциальной информацией данного Пользователя ПлЦР. ПУЦ не осуществляет хранение ключей ЭП Пользователя ПлЦР.

Персональная и корпоративная информация о Пользователе ПлЦР, хранящаяся в ПУЦ, не являющаяся общедоступной в связи с включением ее в Сертификат, считается конфиденциальной.

Реестры ПУЦ, за исключением реестра Сертификатов и реестра аннулированных Сертификатов, являются конфиденциальной информацией ПУЦ и относятся к коммерческой тайне.

Отчет о проведении проверки подлинности ЭП в электронном документе, выполненной по Заявлению на проверку подлинности электронной подписи в электронном документе, является конфиденциальной информацией ПУЦ.

ПУЦ имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных действующим законодательством Российской Федерации.

7.2. Типы информации, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

Открытая информация может публиковаться по решению ПУЦ. Место, способ и время публикации открытой информации определяется ПУЦ.

Персональные данные, включаемые в сертификаты Пользователей ПлЦР и САС, издаваемые ПУЦ, подлежат включению в общедоступный источник персональных данных – Реестр Сертификатов и аннулированных Сертификатов во исполнение обязанности ПУЦ, возложенной на него п.п.5, 6 ч.1 ст.13 Федерального закона № 63-ФЗ.

Обработка персональных данных ПУЦ осуществляется в целях выдачи сертификата, выпуска САС и обеспечения работоспособности и информационной целостности инфраструктуры ПУЦ.

Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

8. РАЗРЕШЕНИЕ СПОРОВ

При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться действующим законодательством Российской Федерации.

Сторонами в споре, в случае его возникновения, считаются Банк, являющийся ПУЦ, и Клиент.

При возникновении споров, стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, и по которым не было достигнуто соглашение, разрешаются в судебном порядке в соответствии с действующим законодательством Российской Федерации.

**Заявление на выдачу сертификата ключа проверки электронной подписи
(физические лица)**

Настоящим, _____
(фамилия, имя, отчество физического лица, его место жительства)
серия _____ № _____, выдан «___» _____ 20__ г.
(наименование документа, удостоверяющего личность)

(кем выдан)

(номер СНИЛС)

(номер мобильного телефона)

1) прошу зарегистрировать меня в Реестрах УЦ АО «АЛЬФА-БАНК», подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России, и изготовить сертификат ключа проверки электронной подписи в соответствии с указанными данными:

Владелец (DN)	
C	RU
O	ID Пользователя ¹
CN	ID ФП ²
L	CBDC
OU	ID СЦР Пользователя ПлЦР ³
STREET	Фамилия Имя Отчество клиента ПлЦР
GN	Пользователь ПлЦР
SNILS	Страховой номер индивидуального лицевого счета в системе обязательного пенсионного страхования у клиента ПлЦР
T	Серия CBDC <серия ключа> ⁴

2) подписанием настоящего заявления, я

(ФИО физического лица)

¹ ID Пользователя – соответствующий идентификатор Пользователя ПлЦР согласно Альбому ЭС

² ID ФП – соответствующий идентификатор ФП, Участника ПлЦР, у которого обслуживается Пользователь ПлЦР согласно Альбому ЭС

³ ID СЦР Пользователя ПлЦР – соответствующий идентификатор СЦР на ПлЦР согласно Альбому ЭС

⁴ серия ключа – содержит то же значение, что и серия ключа в сертификате подчиненного центра сертификации ФП, на котором выпущен сертификат Клиента

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие Акционерному обществу (АО) «АЛЬФА-БАНК» (юридический адрес 107078, г. Москва, ул. Каланчевская, д. 27) на обработку персональных данных: паспортные данные (фамилия, имя, отчество, пол, серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации), СНИЛС, адрес места жительства, номер мобильного телефона, включая следующие виды обработки: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение с использованием средств автоматизации и без использования таких средств, а также путём смешанной обработки.

Настоящее согласие на обработку персональных данных дается в целях исполнения функций удостоверяющего центра АО «АЛЬФА-БАНК» по созданию, выдаче и аннулированию сертификатов ключей проверки электронной подписи (далее - Сертификат) в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» (далее – Федеральный закон №63-ФЗ).

Выражаю согласие на внесение указанных в настоящем заявлении данных в общедоступный источник персональных данных - Реестр Сертификатов и аннулированных Сертификатов, во исполнение обязанностей, возложенных на удостоверяющий центр п.п.5, 6 ч. 2 ст. 13 Федерального закона №63-ФЗ. Я проинформирован и даю согласие на предоставление АО «АЛЬФА-БАНК» любому лицу по его обращению информации, содержащейся в указанном Реестре, в том числе информацию об аннулировании Сертификатов.

Я проинформирован, что настоящее согласие на обработку персональных данных вступает в силу со дня его подписания. Согласие действует в течение срока действия Сертификата. После истечения срока действия согласия удостоверяющий центр АО «АЛЬФА-БАНК» вправе осуществлять обработку персональных данных в случаях, предусмотренных действующим законодательством. Согласие на обработку персональных данных может быть отозвано мной в письменной форме с одновременным аннулированием Сертификата путем обращения в АО «АЛЬФА-БАНК». При этом АО «АЛЬФА-БАНК» вправе осуществлять хранение и уничтожение персональных данных в течение срока хранения документов, установленного законодательством об архивном делопроизводстве.

Подписанием настоящего заявления,

(ФИО физического лица)

присоединяется к Регламенту Удостоверяющего центра АО «АЛЬФА-БАНК», подчиненного подсистеме Удостоверяющего центра платформы цифрового рубля Банка России, в соответствии со ст. 428 ГК РФ.

(Место для штампа ЭП Пользователя ПлЦР)

Заявление на выдачу сертификата ключа проверки электронной подписи (юридические лица)

Настоящим, _____
(фамилия, имя, отчество физического лица – представителя юридического лица, его место жительства)
_____ серия _____ № _____, выдан «___» _____ 20__ г.
(наименование документа, удостоверяющего личность)

(кем выдан)

(номер СНИЛС)

(номер мобильного телефона)
являющийся представителем _____
(наименование и местонахождение юридического лица)

1) прошу зарегистрировать меня в Реестрах УЦ АО «АЛЬФА-БАНК», подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России, и изготовить сертификат ключа проверки электронной подписи в соответствии с указанными данными:

Владелец (DN)	
C	RU
O	ID Пользователя ⁵
CN	ID ФП ⁶
L	CBDC
OU	ID СЦР Пользователя ПлЦР ⁷
STREET	Наименование и место нахождения юридического лица – клиента ПлЦР и, при необходимости, физическое лицо, действующее от имени юридического лица
GN	Пользователь ПлЦР
SNILS	Страховой номер индивидуального лицевого счета в системе обязательного пенсионного страхования у клиента ПлЦР
T	Серия CBDC <серия ключа> ⁸

⁵ ID Пользователя – соответствующий идентификатор Пользователя ПлЦР согласно Альбому ЭС

⁶ ID ФП – соответствующий идентификатор ФП, Участника ПлЦР, у которого обслуживается Пользователь ПлЦР согласно Альбому ЭС

⁷ ID СЦР Пользователя ПлЦР – соответствующий идентификатор СЦР на ПлЦР согласно Альбому ЭС

⁸ серия ключа – содержит то же значение, что и серия ключа в сертификате подчиненного центра сертификации ФП, на котором выпущен сертификат Клиента

2) подписанием настоящего заявления, я

(ФИО физического лица – представителя юридического лица)

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие Акционерному обществу (АО) «АЛЬФА-БАНК» (юридический адрес 107078, г. Москва, ул. Каланчевская, д. 27) на обработку персональных данных: паспортные данные (фамилия, имя, отчество, пол, серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации), СНИЛС, адрес места жительства, номер мобильного телефона, должность, место работы, включая следующие виды обработки: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение с использованием средств автоматизации и без использования таких средств, а также путём смешанной обработки.

Настоящее согласие на обработку персональных данных дается в целях исполнения функций удостоверяющего центра АО «АЛЬФА-БАНК» по созданию, выдаче и аннулированию сертификатов ключей проверки электронной подписи (далее - Сертификат) в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» (далее – Федеральный закон №63-ФЗ).

Выражаю согласие на внесение указанных в настоящем заявлении данных в общедоступный источник персональных данных - Реестр Сертификатов и аннулированных Сертификатов, во исполнение обязанностей, возложенных на удостоверяющий центр п.п.5, 6 ч. 2 ст. 13 Федерального закона №63-ФЗ. Я проинформирован и даю согласие на предоставление АО «АЛЬФА-БАНК» любому лицу по его обращению информации, содержащейся в указанном Реестре, в том числе информацию об аннулировании Сертификатов.

Я проинформирован, что настоящее согласие на обработку персональных данных вступает в силу со дня его подписания. Согласие действует в течение срока действия Сертификата. После истечения срока действия согласия удостоверяющий центр АО «АЛЬФА-БАНК» вправе осуществлять обработку персональных данных в случаях, предусмотренных действующим законодательством. Согласие на обработку персональных данных может быть отозвано мной в письменной форме с одновременным аннулированием Сертификата путем обращения в АО «АЛЬФА-БАНК». При этом АО «АЛЬФА-БАНК» вправе осуществлять хранение и уничтожение персональных данных в течение срока хранения документов, установленного законодательством об архивном делопроизводстве.

Подписанием настоящего заявления,

(ФИО физического лица – представителя юридического лица)

присоединяется к Регламенту Удоcтoвeряющeгo цeнтpa AO «AЛbФa-BAHК», подчиненного подсистеме Удоcтoвeряющeгo цeнтpa платформы цифрового рубля Банка России, в соответствии со ст. 428 ГК РФ.

(Место для штампа ЭП Пользователя ПлЦР)

Заявление на аннулирование сертификата ключа проверки электронной подписи

Настоящим _____
(фамилия, имя, отчество заявителя, его место жительства)
_____ серия _____ № _____, выдан «__» _____ 20__
г.
(наименование документа, удостоверяющего личность)

(кем выдан)
просит аннулировать сертификат ключа проверки электронной подписи
серийный номер _____
сертификата: _____,
выданный на имя/организацию _____,
(фамилия, имя, отчество клиента – физического лица/наименование и место нахождения клиента -
юридического лица и фамилия, имя, отчество представителя клиента)
для _____
, _____ (id Клиента в Платформе ЦР)
по причине _____

(подпись) (расшифровка подписи)
«__» _____ 20__ г.

Заявление на проверку подлинности электронной подписи в электронном документе

Настоящим, _____
(фамилия, имя, отчество Заявителя, его место жительства)
серия _____ № _____, выдан «__» _____ 20__

г. _____
(наименование документа, удостоверяющем личность)

_____ (кем выдан)

1) просит проверить подлинность электронной подписи в электронном документе на основании следующих данных:

- файла сертификата ключа проверки электронной подписи подписанта отмеченного электронного документа;
- файла оспариваемого электронного документа с ЭП/реквизитов оспариваемого электронного документа;
- даты и времени, на момент наступления которых требуется подтвердить подлинность электронной подписи: «__» _____ 20__ г. ____ ч. ____ мин. по московскому времени.

(если дата и время не указаны, то подлинность электронной подписи устанавливается на дату принятия заявления Банком);

2) подписанием настоящего заявления,

я _____
(ФИО физического лица – представителя юридического лица)

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие Акционерному обществу (АО) «АЛЬФА-БАНК» (юридический адрес 107078, г. Москва, ул. Каланчевская, д. 27) соглашаюсь на обработку персональных данных: паспортные данные (фамилия, имя, отчество, пол, серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации), СНИЛС, адрес места жительства, номер мобильного телефона, должность, место работы, включая следующие виды обработки: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение с использованием средств автоматизации и без использования таких средств, а также путём смешанной обработки.

Настоящее согласие на обработку персональных данных дается в целях исполнения функций удостоверяющего центра АО «АЛЬФА-БАНК» по проверке подлинности ЭП в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

Я проинформирован, что настоящее согласие на обработку персональных данных вступает в силу со дня его подписания. Согласие действует до достижения целей обработки персональных данных. После истечения срока действия согласия удостоверяющий центр АО «АЛЬФА-БАНК» вправе осуществлять обработку персональных данных в случаях, предусмотренных действующим законодательством. Согласие на обработку персональных данных может быть отозвано мной в письменной форме путем обращения в АО «АЛЬФА-БАНК».

Субъект персональных данных _____
(подпись) (расшифровка подписи)

«__» _____ 20__ г.

Прошу уведомить меня о дате, времени и месте проведения технической экспертизы по проверке подлинности ЭП под электронным документом следующим способом: _____

Заявитель: _____

(подпись) (расшифровка подписи)

« ____ » _____ 20__ г.

Руководство по обеспечению безопасности использования ключей электронной подписи и средств электронной подписи

1. Общие положения

Настоящее Руководство подготовлено в соответствии с частью 2 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и предназначено для официального информирования владельцев сертификатов ключей проверки электронной подписи (далее - Сертификат), выдаваемых Удостоверяющим центром АО «АЛЬФА-БАНК», подчиненным подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (далее – ПУЦ), о рисках, условиях и правилах применения электронной подписи (далее – ЭП) и средств ЭП, а также о мерах, необходимых для обеспечения безопасности использования ЭП и средств ЭП.

При использовании в правоотношениях ЭП, использовании и эксплуатации средств ЭП владельцы Сертификатов и средств ЭП должны соблюдать требования:

- Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- 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, утвержденной приказом ФАПСИ от 13.06.2001 № 152;
- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66;
- эксплуатационной документации на средства ЭП;
- Регламента Удостоверяющего центра АО «АЛЬФА-БАНК», подчиненного подсистеме Удостоверяющего центра платформы Цифрового рубля Банка России (далее – Регламент);
- настоящего Руководства.

2. Риски, связанные с использованием ЭП

К основным рискам, связанным с использованием ЭП, относятся:

2.1. Несанкционированное подписание электронного документа ЭП, которое может быть произведено в результате:

- компрометации ключа ЭП;
- подмены подписываемого электронного документа в результате работы на компьютере или мобильном устройстве вредоносного программного обеспечения.

2.2. Негативные последствия, вызванные невозможностью подписания электронного документа ЭП, обусловленной следующими событиями:

- уничтожение (удаление с ключевого носителя) ключа ЭП и (или) Сертификата;
- блокировка доступа к ключу ЭП, вызванная неоднократным вводом некорректного кода доступа (пароля или ПИН-кода);
- физическая утрата ключевого носителя.

3. Меры защиты ключей ЭП

Ключи ЭП рекомендуется защищать паролем (ПИН-кодом).

Ответственность за обеспечение конфиденциальности пароля (ПИН-кода) и ключа ЭП возлагается на владельца ключа ЭП.

4. Обращение с ключами ЭП

Ключи ЭП должны использоваться только владельцем ключа ЭП и храниться с исключением возможности его бесконтрольного использования.

Запрещается:

- передавать ключи ЭП третьим лицам;
- сообщать ПИН - код к ключам ЭП третьим лицам;
- записывать ПИН - код к КН на бумажном носителе или запоминать его в программах;
- осуществлять несанкционированное копирование ключей ЭП.

5. Владелец Сертификата обязан:

- обеспечить конфиденциальность ключа ЭП;
- принять меры по исключению несанкционированного доступа к ключам ЭП;
- применять для формирования ЭП только действующий ключ ЭП;
- не использовать ключ ЭП и немедленно обратиться в ПУЦ для прекращения действия Сертификата при наличии оснований полагать, что конфиденциальность ключа ЭП нарушена;
- не использовать ключ ЭП, связанный с Сертификатом, заявление, на прекращение действия которого подано в ПУЦ;
- осуществлять контроль сроков действия Сертификата.

6. Компрометация ключа ЭП

Под компрометацией ключа ЭП понимается утрата доверия к тому, что используемые ключи ЭП обеспечивают безопасность информации. Компрометация ключей ЭП происходит, как правило, вследствие событий:

- потеря ключевого носителя либо потеря ключевого носителя с его последующим обнаружением;
- получение доступа к ключам ЭП неуполномоченных лиц;
- подозрения на утечку информации или её искажение при обмене электронными документами.

7. Действия при компрометации ключей ЭП

Владелец Сертификата самостоятельно должен определить факт компрометации ключа ЭП, оценить значение такого события и выполнить мероприятия по локализации последствий компрометации ключа ЭП.

При компрометации ключа ЭП Владелец Сертификата должен немедленно инициировать мероприятия по аннулированию Сертификата в порядке, установленном Регламентом.