

**Приложение к Распоряжению
от 07.04.2025 г. № 1360**

**РЕГЛАМЕНТ
Удостоверяющего центра АО «АЛЬФА-БАНК»**

Версия 2

Москва 2025

ИСТОРИЯ ВЕРСИЙ	
Версия №	Дата и № Приказа/Распоряжения
1	3888 от 20.12.2023
2	1360 от 07.04.2025

Оглавление

1. Термины и определения.....	4
2. ОБЩИЕ ПОЛОЖЕНИЯ	7
3. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ 8	
4. ПРАВА И ОБЯЗАННОСТИ СТОРОН	8
5. ПРАВИЛА ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	11
6. УПРАВЛЕНИЕ СЕРТИФИКАТАМИ В УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ	14
7. КОНФИДЕНЦИАЛЬНОСТЬ.....	16
8. РАЗРЕШЕНИЕ СПОРОВ	16
9. ОТВЕТСТВЕННОСТЬ СТОРОН	16
Приложение № 1	18
Приложение №2а	20
Приложение №2б	22
Приложение №2в	24
Приложение №2г	25
Приложение № 2д	26
Приложение № 3	27
Приложение № 4	29
Приложение № 5	31

1. Термины и определения

Администратор УЦ – ответственный работник Удостоверяющего Центра, в соответствии с должностными обязанностями наделенный полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей подписей Операторов и Пользователей Удостоверяющего Центра и уполномоченный Удостоверяющим Центром расписываться собственноручной подписью в Сертификатах на бумажном носителе, выданных Удостоверяющим центром.

Банк – АО «АЛЬФА-БАНК».

Бизнес-система – обобщенное понятие корпоративной информационной системы, эксплуатирующейся в Банке, или внешней информационной системы при условии предварительного согласования с УЦ порядка выдачи Сертификатов для работы в данной Бизнес-системе, в которой используются ключи электронной подписи и сертификаты ключей проверки электронной подписи, и предоставляющей определенные услуги пользователям – участникам этой системы.

Владелец сертификата ключа проверки электронной подписи (Владелец сертификата) – лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке выдан сертификат.

Договор на обслуживание в Бизнес-системе (договор на обслуживание) – договор, заключенный между юридическим лицом или индивидуальным предпринимателем и Банком на пользование услугами (обслуживание) в Бизнес-системе.

Заявитель – лицо, обращающееся 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. В рамках настоящего Регламента Заявителем может быть юридическое лицо и/или физическое лицо - представитель юридического лица.

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

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

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем Ключа электронной подписи и Ключа проверки электронной подписи.

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.

Область действия сертификата ключа проверки электронной подписи – включенные в сертификат ключа проверки электронной подписи сведения об отношениях, при которых электронный документ с электронной подписью, созданной с использованием соответствующего сертификата ключа проверки электронной подписи, будет иметь юридическое значение.

Оператор УЦ – уполномоченный работник Банка, наделенный Удостоверяющим центром полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей подписей Пользователей Удостоверяющего центра, а также правом расписываться собственноручной подписью на копиях сертификатов ключей подписей Пользователей Удостоверяющего центра (заверять копии сертификатов ключей подписей).

Пользователь Бизнес-системы – представитель юридического лица, заключившего договор на обслуживание в Бизнес-системе; работник Банка, получивший доступ в Бизнес-систему в рамках своих должностных обязанностей; Банк, использующий Сертификат для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе или Сертификат безопасности.

Пользователь Удостоверяющего Центра (Пользователь) – Пользователь Бизнес-системы, присоединившийся к Регламенту Удостоверяющего Центра, внесенный в реестр Удостоверяющего Центра.

Реестр Удостоверяющего Центра – набор документов Удостоверяющего Центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений пользователей на изготовление Сертификата;
- реестр зарегистрированных пользователей Удостоверяющего Центра;
- реестр запросов на сертификат ключа проверки электронной подписи;
- реестр заявлений на аннулирование (отзыв) сертификата ключа проверки электронной подписи;
- реестр выданных и аннулированных сертификатов ключей проверки электронной подписи;
- реестр изготовленных списков отозванных сертификатов;
- служебные документы Удостоверяющего Центра.

Сертификат безопасности – сертификат по формату X.509, используемый для организации защищенного TLS соединения. УЦ выдает Сертификаты безопасности Банку и/или работнику Банка для использования в корпоративных Бизнес-системах. **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. УЦ выдает следующие Сертификаты:

- Сертификат юридического лица на работника Банка, используемый для подписания документов от лица Банка. Владельцами такого Сертификата являются Банк и работник Банка;
- Сертификат юридического лица, заключившего договор на обслуживание в Бизнес-системе, на представителя юридического лица. Владельцами такого Сертификата являются юридическое лицо и представитель юридического лица;
- Сертификат, используемый для автоматического создания и (или) автоматической проверки электронных подписей в корпоративных Бизнес-системах (Обезличенный сертификат). Владельцем такого Сертификата является Банк.

Список отозванных сертификатов (СОС) – 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 приостановлено. Момент времени формирования списка отозванных сертификатов определяется по значению поля «Действителен с» списка отозванных сертификатов.

Средства удостоверяющего центра – программное и (или) аппаратное средство, используемое для реализации функций удостоверяющего центра.

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.

Удостоверяющий Центр Банка (Удостоверяющий Центр или УЦ) – функциональное подразделение Банка, осуществляющее функции по созданию и выдаче неквалифицированных Сертификатов, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Уполномоченный представитель – физическое лицо, наделенное юридическим лицом или индивидуальным предпринимателем полномочиями на получение и пользование услугами Удостоверяющего Центра.

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 и Бизнес-системы Банка осуществляют 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.

Internet Assigned Numbers Authority (IANA, ассоциация IANA) – международная организация, координирующая выделение объектных идентификаторов, предназначенных для идентификации телекоммуникационных объектов.

63-ФЗ – Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Предмет Регламента

2.1.1. Настоящий Регламент Удостоверяющего центра АЛЬФА-БАНК (далее – Регламент) определяет условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Удостоверяющего центра и Пользователей, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего Центра.

2.1.2. Удостоверяющий центр осуществляет целевые функции по созданию и выдаче неквалифицированных сертификатов ключей проверки электронной подписи и иные функции удостоверяющего центра в соответствии с требованиями действующей редакции 63-ФЗ и иными принимаемыми в соответствии с ним правовыми актами.

2.1.3. Любое заинтересованное лицо может ознакомиться с Регламентом Удостоверяющего центра, который размещен на сайте Удостоверяющего центра в сети «Интернет» по адресу: <http://cdp.alfabank.ru/>.

2.2. Сведения об Удостоверяющем центре

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

2.2.3. Сокращенное наименование: АО «АЛЬФА-БАНК»

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

2.2.5. УЦ осуществляет свою работу в круглосуточном режиме.

2.2.6. График работы УЦ по созданию и выдаче сертификатов: ПН-ПТ — с 10.00 до 17.00, обед — с 12.00 до 12.45; СБ-ВС — выходной.

2.3. Порядок информирования о предоставлении услуг УЦ

2.3.1. Информирование об осуществлении функций УЦ доступно следующими способами:

- тел./факс: +7 (495) 620-91-91;
- e-mail: nCA@alfabank.ru;
- сайт УЦ в сети «Интернет»: <http://cdp.alfabank.ru/>

2.4. Условия оказания услуг УЦ

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 УЦ, должно рассматриваться всеми заинтересованными лицами как публичное предложение (оферта) со стороны Банка заключить договор о предоставлении услуг УЦ, существенные условия которого содержатся в настоящем Регламенте.

2.4.3. Услуги УЦ могут быть оказаны только пользователям Бизнес-систем, приведенных в Приложении № 1 к настоящему Регламенту. Для добавления новой Бизнес-системы с уникальными областями действия Сертификатов в Приложение №1 необходимо предварительно согласовать с УЦ порядок выдачи Сертификатов для работы в данной Бизнес-системе.

2.4.4. Нормы, содержащиеся в Регламенте, становятся обязательными для Пользователя с момента подписания и предоставления в УЦ Заявления на изготовление Сертификата (далее – Заявление) по форме Приложения № 2 к настоящему Регламенту.

2.4.5. С момента подачи в УЦ Заявления Заявитель, считается присоединившимся к

Регламенту и является Стороной Регламента.

2.4.6. Требования настоящего Регламента распространяются на Владельца сертификата в течение срока действия Сертификата.

2.4.7. Стороны согласны с тем, что условия настоящего Регламента принимаются Пользователем полностью без каких-либо изъятий, изменений и протоколов разногласий.

2.4.8. Владелец сертификата имеет право в одностороннем порядке прекратить взаимодействие с УЦ в рамках Регламента, направив в УЦ заявление на прекращение действия выданного ему Сертификата.

2.5. Внесение изменений в Регламент УЦ

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

2.5.2. Уведомление о внесении изменений или дополнений в Регламент осуществляется путем размещения соответствующей информации на сайте УЦ в сети "Интернет": <http://cdp.alfabank.ru/>.

2.5.3. Все изменения (дополнения), вносимые УЦ 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 УЦ по адресу - <http://cdp.alfabank.ru/>.

2.5.4. Все изменения (дополнения), вносимые УЦ 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 случае, если Пользователь не согласен со внесенными изменениями и дополнениями он имеет право прекратить использование сертификата, в порядке, предусмотренном п. 5.4.5 настоящего Регламента.

3. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ

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

- 3.1. Создание и выдача сертификатов.
- 3.2. Подтверждение владения Заявителем ключом ЭП, соответствующим ключу проверки ЭП, указанному им для получения сертификатов.
- 3.3. Установление сроков действия сертификатов.
- 3.4. Аннулирование выданных УЦ сертификатов.
- 3.5. Выдача средств ЭП.
- 3.6. Ведение реестра УЦ.
- 3.7. Проверка уникальности ключей проверки ЭП в Реестре сертификатов.
- 3.8. Проверка действительности ЭП по обращениям Заявителей.
- 3.9. Осуществление иной деятельности, предусмотренной 63-ФЗ.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Удостоверяющий центр имеет право:

4.1.1. Наделить Оператора УЦ полномочиями по осуществлению действий по регистрации и управлению сертификатами Пользователей, а также правом расписываться собственноручной подписью на копиях сертификатов Пользователей (заверять копии сертификатов).

4.1.2. Выдавать сертификат как в форме электронных документов, так и в форме документов на бумажном носителе.

4.1.3. Отказать Заявителю, в случае несоблюдения требованиям. Указанным в п. 2.4.4, в выдаче Сертификата.

4.1.4. Запрашивать у заявителя документы для подтверждения достоверности представленных им сведений, содержащихся в Заявлении.

4.1.5. Дополнительно подтверждать достоверность сведений в отношении заявителя одним из следующих способов:

- с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;
- информационных систем органов государственной власти, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата, единой государственного реестра налогоплательщиков;
- с использованием Бизнес-Системы, пользователем которой он является.

4.1.6. Отказать заявителю в создании и выдаче Сертификата в случае:

- не соответствия требованиям настоящего Регламента или договора на обслуживание в Бизнес-системе в части выпуска Сертификата;
- непредставления документов для создания и выдачи Сертификата, или оформления их ненадлежащим образом;
- отсутствия подтверждения из государственных информационных ресурсов достоверности информации, представленной заявителем для включения в Сертификат;
- не идентифицирована личность Заявителя;
- отсутствия поддержки со стороны УЦ СКЗИ, применяемого Пользователем для формирования запроса на сертификат.

4.1.7. Отказать в аннулировании (отзыве) сертификата Пользователя в случае, если истек установленный срок действия ключа ЭП, соответствующего этому Сертификату.

4.1.8. Аннулировать (отозвать) сертификат Пользователя в случае обращения Пользователя по следующим основаниям:

- компрометации или подозрений в компрометации ключа ЭП;
- изменения данных Пользователя в Сертификате;
- прекращения/ограничения доступа в Бизнес-систему;
- нарушения Пользователем положений Регламента;
- получения заявления на прекращение действия сертификата;
- поступления в УЦ информации о смерти Владельца;
- прекращения деятельности УЦ без перехода его функций другим лицам;
- в иных случаях, предусмотренных действующим законодательством и настоящим Регламентом.

4.1.9. Самостоятельно устанавливать порядок реализации функций УЦ, осуществления его прав и исполнения обязанностей, определенных ст. 13 63-ФЗ.

4.2. Удостоверяющий центр обязан:

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

4.2.2. Обеспечить регистрацию Пользователей по заявлениям на создание Сертификата в соответствии с порядком регистрации, изложенным в настоящем Регламенте.

4.2.3. Обеспечить изготовление Сертификата зарегистрированного пользователя в соответствии с порядком, определенным в настоящем Регламенте.

4.2.4. Обеспечить уникальность серийных номеров изготавливаемых Сертификатов Пользователей, а также значений ключей проверки ЭП.

4.2.5. Аннулировать (отозвать) сертификат по заявлению на аннулирование (отзыв) сертификата, поступающему от Владельца сертификата, а также по основаниям, указанным в ч.6. и 6.1 ст.14 63-ФЗ, и в течение двенадцати часов с момента наступления указанных обстоятельств, занести сведения об аннулированном (отозванном) Сертификате в СОС с указанием даты и времени занесения и причины отзыва.

4.2.6. Официально уведомлять об аннулировании и прекращении, действия сертификата всех лиц, зарегистрированных в УЦ, посредством публикации СОС.

4.2.7. Публиковать актуальный СОС не позднее 1 (одного) часа с момента его создания, на сайте УЦ в сети «Интернет» по адресу <http://cdp.alfabank.ru/>.

4.2.8. Отказать заявителю в создании сертификата в случаях:

- если не было подтверждено то, что заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному заявителем для получения сертификата;
- отрицательного результата проверки в реестре сертификатов уникальности регистрационных данных, указанных заявителем для получения сертификата.

4.2.9. Вести реестр сертификатов.

4.3. Пользователь обязан.

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

4.3.2. Извещать УЦ обо всех изменениях данных, внесенных в Сертификат.

4.3.3. При подаче Заявления указать действующий электронный почтовый адрес Владельца сертификата для получения извещений, уведомлений от УЦ, связанных с применением Сертификата, его аннулированием.

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

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

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

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

4.3.8. Не использовать Ключ ЭП, связанный с Сертификатом, заявление на аннулирование (отзыв) которого подано в УЦ.

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

4.3.10. Регулярно, не реже чем один раз в 5 дней, просматривать страницу УЦ в сети «Интернет», расположенную по адресу <http://cdp.alfabank.ru/> на предмет изменения Регламента.

4.4. Пользователь УЦ имеет право.

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

4.4.2. Получить Сертификат как в форме электронных документов, так и в форме документов на бумажном носителе.

4.4.3. Получить информацию о статусе Сертификата и подтверждение его владением на определенный момент времени.

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

5. ПРАВИЛА ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

5.1. Регистрация пользователей

5.1.1. Порядок регистрации пользователей Бизнес-систем Банка в УЦ изложен в приложениях к настоящему Регламенту, которые описывают процедуры регистрации пользователей, генерации ключей, управления сертификатами применительно к этим Бизнес-системам.

5.2. Генерация ключей

5.2.1. Порядок генерации ключей ЭП пользователей в Бизнес-системах Банка изложен в приложениях к настоящему Регламенту, которые описывают процедуры регистрации пользователей, генерации ключей, управления сертификатами применительно к этим Бизнес-системам.

5.3. Изготовление и получение Сертификата

5.3.1. Создание и выдача Сертификата осуществляется УЦ на основании Заявления по форме Приложений № 2а-2в к настоящему Регламенту, если иное не установлено требованиями Бизнес-системы.

Актуальные формы Заявлений определяются УЦ самостоятельно. УЦ вправе вносить в них любые изменения по своей инициативе без уведомления Пользователей.

Заявление может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного электронной подписью в соответствии с требованиями 63-ФЗ.

В случае, если в УЦ обращается Заявитель - представитель стороннего юридического лица, к Заявлению прилагается доверенность на обращение в УЦ по форме Приложения №2г к настоящему Регламенту.

В случае, если обращается Заявитель - представитель Банка, к Заявлению прилагается организационно-распорядительный документ по форме Банка о наделении Заявителя полномочиями по работе с усиленной неквалифицированной электронной подписью (УНЭП).

5.3.2. УЦ проверяет данные в Заявлении на соответствие данным, содержащимся в иных представленных Заявителем документах, и устанавливает:

- факт принадлежности документов предоставившему их лицу;
- факт соответствия сведений, указанных в заявлении, представленным документам и информации;
- факт отсутствия признаков подделки документов.

5.3.3. Поскольку в Сертификат подлежат включению персональные данные Заявителя, Заявитель предоставляет свое согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия включен в Заявление. Согласие должно быть подписано лицом, данные о котором вносятся в Сертификат (субъектом персональных данных).

5.3.4. При подаче заявления осуществляется идентификация Заявителя в соответствии с положениями статьи 13 63-ФЗ.

5.3.5. При получении Сертификата УЦ ознакомливает Владельца сертификата с информацией, содержащейся в Сертификате. Подтверждение ознакомления с информацией, содержащейся в неквалифицированном сертификате, осуществляется под расписку.

5.3.6. Индивидуальный порядок изготовления и получения Сертификатов изложен в приложениях к настоящему Регламенту, которые описывают процедуры регистрации пользователей, генерации ключей, управления сертификатами применительно к этим Бизнес-системам. В случае разногласий между положениями п.5.3 Регламента и соответствующим приложением, приоритетными считаются условия, указанные в приложении.

5.3.7. Порядок изготовления и получения Сертификатов безопасности изложен в Приложении №4 к настоящему Регламенту. Пункты 5.3.1-5.3.6 на Сертификаты безопасности не распространяются.

5.4. Аннулирование (отзыв) сертификата

5.4.1. Сертификат прекращает свое действие в следующих случаях:

- на основании заявления Владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- по истечении установленного срока его действия;
- в случаях, предусмотренных правилами Бизнес-системы и описанных в соответствующих приложениях к Регламенту;
- в иных случаях, установленных 63-ФЗ, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и Владельцем сертификата.

5.4.2. УЦ признает Сертификат аннулированным 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.

5.4.3. 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 УЦ в СОС.

5.4.4. В случае компрометации ключа ЭП УЦ временем аннулирования (отзыва) сертификата Пользователя признается время компрометации ключа ЭП УЦ, фиксирующееся в реестре УЦ. В случае компрометации ключа ЭП УЦ информация о сертификате Пользователя в СОС не заносится.

5.4.5. Аннулирование Сертификата по заявлению Пользователя:

Для осуществления аннулирования (отзыва) Сертификата пользователь подает заявление на аннулирование (отзыв) сертификата в УЦ на бумажном носителе или в форме электронного документа через Бизнес-систему.

5.4.6. Заявление на аннулирование Сертификата на бумажном носителе оформляется по форме, утвержденной Приложением №2д к Регламенту.

5.4.7. Заявление на аннулирование Сертификата, подаваемого в форме электронного документа через Бизнес-систему должно содержать следующую информацию:

- идентификационные данные Владельца сертификата;
- наименование Бизнес-системы;
- серийный номер отзываемого Сертификата;
- причина отзыва Сертификата;
- дата и время подачи заявления.

5.4.8. Порядок формирования и передачи заявления на аннулирование (отзыв) сертификата в электронном виде в конкретной Бизнес-системе Банка приводится в

приложении к настоящему Регламенту, описывающему процедуры управления сертификатами в этой Бизнес-системе (если такая услуга предоставляется в Бизнес-системе).

5.4.9. Подача заявления на аннулирование (отзыв) Сертификата, оформленного в бумажном виде, в УЦ и его рассмотрение осуществляется в течение одного рабочего дня.

5.4.10. Официальным уведомлением о факте отзыва Сертификата является опубликование первого (наиболее раннего) СОС, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем отзыва Сертификата признается время издания указанного СОС, хранящееся в поле *thisUpdate* СОС.

5.4.11. Информация о размещении СОС заносится в изданные УЦ Сертификаты в расширение *CRL Distribution Point* Сертификата.

5.4.12. Порядок аннулирования Сертификатов безопасности изложен в приложениях к настоящему Регламенту, которые описывают процедуры управления сертификатами применительно к конкретным Бизнес-системам.

5.5. Подтверждение подлинности ЭП в электронных документах

5.5.1. Подтверждение подлинности ЭП в электронных документах, циркулирующих в Бизнес-системах, осуществляется на основании заявления в свободной форме, в том числе поступающего по установленным правилам Бизнес-системы.

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

5.5.3. Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является предоставление информации, содержащей:

- дата и время подачи заявления;
- наименование Бизнес-системы;
- идентификационные данные субъекта, ЭП которого требуется проверить в электронном документе;
- проверяемый Сертификат;
- область применения Сертификата, указанную в Приложении № 2, если такая область содержится в Сертификате;
- дата и время формирования ЭП в электронном документе;
- файл электронного документа и ЭП к данному документу.

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

5.5.5. В ходе проведения работ УЦ может быть запрошена дополнительная информация.

5.5.6. Процедура подтверждения действительности ЭП осуществляется с использованием специализированного программного обеспечения, входящего в состав средства УЦ, уполномоченными лицами УЦ.

5.5.7. 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 УЦ, проверку действительности всех сертификатов на момент проверки и отсутствие их в СОС.

5.5.8. 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 Заявителем для проведения проверки;
- время и место проведения проверки;

- содержание и результат проверки каждого Сертификата в цепочке до корневого Сертификата УЦ;
- обоснование результатов проверки.

5.5.9. Заключение/протокол проверки ЭП в электронном документе составляется в произвольной форме в двух экземплярах, подписывается уполномоченными лицами УЦ и заверяется печатью. Один экземпляр - предоставляется Заявителю, второй экземпляр - хранится в УЦ.

6. УПРАВЛЕНИЕ СЕРТИФИКАТАМИ В УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

6.1. Порядок смены ключей ЭП УЦ

6.1.1. Смена ключа ЭП УЦ осуществляется в связи с истечением срока его действия (далее – плановая смена ключа ЭП).

6.1.2. Плановая смена ключей ЭП УЦ выполняется в период действия ключа ЭП УЦ.

6.1.3. Процедура плановой смены ключей ЭП УЦ осуществляется в следующем порядке:

- УЦ формирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- УЦ изготавливает сертификат нового ключа проверки ЭП и подписывает его ЭП с использованием нового ключа ЭП.

6.1.4. При плановой смене ключа ЭП УЦ все Владельцы сертификатов должны установить на своих компьютерах новый сертификат УЦ.

6.1.5. Информирование Владельцев сертификатов о проведении плановой смене ключа уполномоченного лица УЦ осуществляется посредством публикации информации на официальном сайте УЦ по адресу: <http://cdp.alfabank.ru/>.

6.1.6. Доверенным способом получения нового сертификата УЦ является его публикация на официальном сайте УЦ по адресу: <http://cdp.alfabank.ru/>, доступная для скачивания.

6.1.7. Старый ключ ЭП УЦ используется в течение своего срока действия для формирования СОС, изданных УЦ в период действия старого ключа ЭП УЦ.

6.2. Компрометация ключа ЭП УЦ

6.2.1. Смена ключа ЭП УЦ осуществляется в случае компрометации ключа ЭП или угрозы компрометации такого ключа ЭП, а также указание на то, что одновременно со сменой такого ключа ЭП прекращается действие всех сертификатов, подписанных с использованием этого ключа ЭП.

6.2.2. Процедура внеплановой смены ключей ЭП УЦ осуществляется не позднее 7 рабочих дней со дня установления факта его компрометации или угрозы его компрометации.

6.2.3. Информирование Владельцев сертификатов о внеплановой смене ключа ЭП УЦ осуществляется путем размещения соответствующей информации на официальном сайте АО «АЛЬФА-БАНК» в сети «Интернет»: <http://cdp.alfabank.ru/> не позднее одного рабочего дня со дня установления факта компрометации ключа ЭП или угрозы его компрометации.

6.2.4. Доверенным способом получения нового сертификата УЦ является его публикация на официальном сайте УЦ по адресу: <http://cdp.alfabank.ru/>, доступная для скачивания и исключающая уничтожение, модифицирование, блокирование при передаче и иные неправомерные действия с сертификатом.

6.3. Компрометация ключа ЭП владельца сертификата

6.3.1. Владелец сертификата самостоятельно принимает решение о факте компрометации или угрозе компрометации своего ключа ЭП.

6.3.2. В случае компрометации или угрозы компрометации ключа ЭП Владелец сертификата подает в УЦ заявление на отзыв сертификата в порядке, установленном разделом 5.4 Регламента.

6.4. Прекращение деятельности УЦ

6.4.1. Прекращение деятельности УЦ может быть осуществлено на основании решения Банка и в порядке, установленном внутренними документами Банка и в соответствии с требованиями 63-ФЗ.

6.4.2. Все сертификаты пользователей, выданные УЦ, аннулируются (отзываются).

6.5. Сроки действия ключей ЭП УЦ

6.5.1. Срок действия ключа ЭП УЦ составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности УЦ, и для средства ЭП, с использованием которого данный ключ ЭП был сформирован.

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

6.5.3. Срок действия сертификата, соответствующего ключу ЭП УЦ, составляет 15 лет.

6.6. Сроки действия ключей ЭП пользователей

6.6.1. Срок действия ключа ЭП Пользователя составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности УЦ, и для средства ЭП, с использованием которого данный ключ ЭП был сформирован.

6.6.2. Начало периода действия ключа ЭП пользователя исчисляется с даты и времени начала действия соответствующего сертификата.

6.6.3. Срок действия сертификата, соответствующего ключу ЭП Пользователя, определяется в приложении к настоящему Регламенту, описывающем процедуры управления сертификатами в этой Бизнес-системе.

6.7. Хранение информации в УЦ

6.7.1. УЦ в течение всего срока своей деятельности, если другие сроки не установлены законодательством Российской Федерации, хранит информацию, внесенную в реестр сертификатов УЦ.

6.7.2. Состав и порядок хранения документов Пользователя определяется в Бизнес-системе.

6.7.3. В случаях отсутствия состава и порядка хранения документов в Бизнес-системе, УЦ может хранить документы, подтверждающие факты оказания услуг УЦ. Документы, подтверждающие факты оказания услуг УЦ, хранятся в течение 5 лет с момента выдачи Сертификата в соответствии с законодательством об архивном деле.

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

6.8. Структура сертификата и СОС

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

6.8.2. Структура сертификата пользователя в конкретной Бизнес-системе Банка может быть приведена в приложении к настоящему Регламенту, описывающему процедуры управления сертификатами в этой Бизнес-системе.

7. КОНФИДЕНЦИАЛЬНОСТЬ

7.1. Типы конфиденциальной информации

7.1.1. Ключ ЭП, соответствующий сертификату пользователя, является конфиденциальной информацией данного пользователя. УЦ не осуществляет хранение ключей ЭП пользователей.

7.1.2. Персональная и корпоративная информация о пользователях, хранящаяся в УЦ, не подлежащая непосредственной рассылке в качестве части сертификата, считается конфиденциальной.

7.2. Типы информации, не являющейся конфиденциальной

7.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

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

7.2.3. Персональные данные, включаемые в сертификаты пользователей и СОС, издаваемые УЦ, относятся к общедоступным персональным данным и могут быть переданы третьим лицам в целях обеспечения работоспособности и информационной целостности инфраструктуры открытых ключей.

7.2.4. Обработка персональных данных УЦ осуществляется в целях выдачи сертификата, выпуска СОС и обеспечения работоспособности и информационной целостности инфраструктуры открытых ключей.

7.2.5. Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

7.3. Исключительные полномочия УЦ

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

8. РАЗРЕШЕНИЕ СПОРОВ

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

8.2. Сторонами в споре, в случае его возникновения, считаются Банк, являющийся УЦ, и пользователь.

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

8.4. 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.

9. ОТВЕТСТВЕННОСТЬ СТОРОН

9.1. Стороны несут ответственность за соблюдение положений настоящего Регламента в соответствии с действующим законодательством Российской Федерации.

9.2. Владелец сертификата несет ответственность за достоверность документов и сведений, предоставляемых в УЦ, неисполнение обязанностей, установленных 63-ФЗ и настоящим Регламентом.

9.3. Удостоверяющий Центр не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие, в связи с этим убытки в случаях:

- подделки, подлога либо иного искажения присоединившейся Стороной, Владелец Сертификата либо третьими лицами информации, содержащейся в заявлении либо иных документах, представленных в УЦ;

- если Владелец Сертификата своевременно не осуществил процедуру по аннулированию (отзыву) Сертификата при компрометации ключа ЭП.

9.4. УЦ несет ответственность за убытки, возникшие вследствие компрометации ключа ЭП УЦ, либо вследствие несоответствия сведений в Сертификате сведениям, указанным в заявлении на выдачу Сертификата.

9.5. Ответственность УЦ регулируется законодательством Российской Федерации.

9.6. Размер ответственности Банка и присоединившейся Стороны при нарушении условий настоящего Регламента определяется в соответствии с договором на обслуживание в Бизнес-системе, подписанным присоединившейся Стороной.

1. Области действия сертификатов ключей проверки электронной подписи

1.1. Принципы построения объектных идентификаторов областей применения сертификатов пользователей.

1.2. В Российском пространстве телекоммуникационных объектных идентификаторов за АО «АЛЬФА-БАНК» зарегистрировано значение 1.2.643.4.3.

1.3. В международной ассоциации IANA за АО «АЛЬФА-БАНК» зарегистрировано значение 1.3.6.1.4.1.16745.

1.4. В качестве корневого объектного идентификатора для построения структуры идентификаторов областей применения сертификатов УЦ используется значение, зарегистрированное в международной ассоциации IANA.

1.5. Структура объектных идентификаторов областей применения сертификатов пользователей имеет вид:

1.3.6.1.4.1.16745.X.YY.ZZZ, где:

- X – Бизнес-система, обозначаемая одним из следующих числовых значений:

1 – Системный раздел

- 20 - Система «Биометрия»;
- YY – область действия сертификата внутри Бизнес-системы;
- ZZZ – область применения сертификата, приведенная в п. 2. настоящего приложения.

1.6. В случае необходимости, для увеличения уровня детализации областей применения сертификатов, возможно введение дополнительного деления объектных идентификаторов, а также использование идентификатора, зарегистрированного в Российском пространстве объектных идентификаторов, для построения дополнительной структуры областей применения сертификатов.

2. Области применения сертификатов Удостоверяющего Центра Банка.

2.1. Технологические области применения сертификатов ключей проверки электронной подписи.

Объектный идентификатор	Название
1.2.643.2.2.34.2	Временный доступ к центру Регистрации
1.2.643.2.2.34.4	Администратор центра Регистрации
1.2.643.2.2.34.5	Оператор центра Регистрации
1.2.643.2.2.34.6	Пользователь центра Регистрации
1.2.643.2.2.34.7	Центр Регистрации

2.2. Области применения сертификатов, относящиеся к Бизнес-системам.

Объектный идентификатор	Название	Область применения
1.3.6.1.4.1.16745.10	Модуль УКС ИС "Целевой Государственной биометрии и ЕСИА"	
1.3.6.1.4.1.16745.10.1	Биометрия. Пользователь	Сертификат с данной областью применения может использоваться

		только для подписи биометрических образцов.
1.3.6.1.4.1.16745.11	Универсальная Бизнес-система	Сертификат с данной областью применения может использоваться только для работы в корпоративных Бизнес-системах работниками Банка и представителями юридического лица, заключившего договор на обслуживание в Бизнес-системе.
1.3.6.1.4.1.16745.12	Сертификаты безопасности (TLS - сертификаты)	Сертификат с данной областью применения может использоваться только для защиты каналов связи в корпоративных Бизнес-системах работниками Банка.

Приложение №2а
к Регламенту Удостоверяющего центра АО «АЛЬФА-БАНК»
Форма заявления на создание и выдачу Сертификата

Для юридических лиц (сотрудники Банка)

Заявление на изготовление неквалифицированного сертификата ключа проверки электронной подписи

АО «АЛЬФА-БАНК»

_____ (полное наименование юридического лица, включая организационно-правовую форму)
в лице _____
_____ (должность уполномоченного лица, фамилия, имя, отчество в родительном падеже)
действующего на основании _____
_____ (реквизиты распоряжения)

просит создать сертификат ключа проверки электронной подписи Уполномоченного представителя Заявителя – юридического лица (Пользователя Удостоверяющего центра АО «АЛЬФА-БАНК») в соответствии с указанными в настоящем заявлении данными *:

Фамилия, Имя, Отчество		
Должность		
СНИЛС		
ИНН ФЛ		
Сокращенное наименование ЮЛ	АО «АЛЬФА-БАНК»	
ИНН / ОГРН	7728168971	1027700067328
Страна / Область	РФ	77 г. Москва
Населенный пункт	г. Москва	
Улица, номер дома, корпус, офис\квартира (если имеется)	ул. Каланчевская, д.27	
Адрес электронной почты		

Я, _____
_____ (фамилия, имя, отчество уполномоченного представителя Заявителя)

паспорт: серия _____ № _____ код подразделения _____ дата выдачи _____ г.

_____ (наименование органа, выдавшего документ)

дата рождения: _____ г., место рождения: _____

Настоящим я свободно, своей волей и в своем интересе даю конкретное, предметное, информированное, однозначное и сознательное согласие на обработку АКЦИОНЕРНЫМ ОБЩЕСТВОМ «АЛЬФА-БАНК» (г. Москва, ул. Каланчевская, д. 27) (далее также – «Банк») следующей информации, относящейся к моим персональным данным, содержащейся в настоящем Заявлении, а также предоставленной мной Банку: фамилия, имя, отчество, СНИЛС, ИНН, контактные данные (мобильный телефон, адрес электронной почты), паспортные данные (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации), место работы, должность.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без использования таких средств, а также путем смешанной обработки персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (предоставление, доступ), блокирование, удаление, уничтожение) в целях исполнения обязательств Удостоверяющего центра АО «АЛЬФА-БАНК» по изготовлению неквалифицированных сертификатов ключей проверки электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Выражаю согласие на внесение указанных в настоящем заявлении данных в реестр сертификатов, обязанность по ведению которого возложена на Удостоверяющий центр согласно ст. 13 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи». Я проинформирован и даю согласие на предоставление АО «АЛЬФА-БАНК» любому лицу по его обращению информации, содержащейся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи, во исполнение обязанности, возложенной на удостоверяющий центр п. 3 ч. 2 ст. 13 указанного Федерального закона.

Настоящее согласие на обработку персональных данных вступает в силу со дня его подписания и действует до достижения целей обработки персональных данных либо до отзыва настоящего согласия. Обработка персональных данных осуществляется в течении срока действия настоящего согласия. После истечения срока действия согласия удостоверяющий центр АО «АЛЬФА-БАНК» вправе осуществлять обработку персональных данных в случаях, предусмотренных действующим законодательством.

Согласие может быть отозвано по письменному заявлению в бумажном виде при личном прибытии Заявителя, при удовлетворении которого впоследствии УЦ аннулируются все выпущенные сертификаты данного Заявителя, при этом УЦ вправе не прекращать обработку персональных данных при наличии иных правовых оснований для продолжения обработки.

Даю согласие на создание сертификата ключа проверки электронной подписи в соответствии со сведениями, указанными в настоящем заявлении. Достоверность данных сведений подтверждаю.

Я проинформирован, что с момента подписания настоящего заявления присоединяюсь к Регламенту удостоверяющего центра АО «АЛЬФА-БАНК».

С настоящим Регламентом и приложениями к нему ознакомлен, полностью и безоговорочно соглашаюсь со всеми его условиями и обязуюсь соблюдать все положения указанного документа.

(Уполномоченный представитель
Заявителя)

(подпись)

(фамилия, инициалы)

« ____ » _____ 20 ____ года

* - обязательны для заполнения и включения в Сертификат поля, содержащие: ФИО владельца сертификата – физического лица, один из идентификаторов (ИНН, СНИЛС), наименование и адрес владельца сертификата – юридического лица.

Приложение №26

к Регламенту Удостоверяющего центра АО «АЛЬФА-БАНК»
Форма заявления на создание и выдачу Сертификата

Для юридических лиц (внешние Заявители)

Заявление на изготовление невалифицированного сертификата ключа проверки электронной подписи

_____ (полное наименование юридического лица, включая организационно-правовую форму)

в лице _____ (должность уполномоченного лица, фамилия, имя, отчество в родительном падеже)

действующего на основании _____ (реквизиты доверенности)

просит создать сертификат ключа проверки электронной подписи Уполномоченного представителя Заявителя – юридического лица (Пользователя Удостоверяющего центра АО «АЛЬФА-БАНК») в соответствии с указанными в настоящем заявлении данными *:

Фамилия, Имя, Отчество			
Должность			
СНИЛС			
ИНН ФЛ			
Сокращенное наименование ЮЛ			
ИНН / КПП / ОГРН			
Страна / Область	РФ		
Населенный пункт			
Улица, номер дома, корпус, офис\квартира (если имеется)			
Адрес электронной почты			

Я, _____ (фамилия, имя, отчество уполномоченного представителя Заявителя)

паспорт: серия _____ № _____ код подразделения _____ дата выдачи _____ г.

_____ (наименование органа, выдавшего документ)

дата рождения: _____ г., место рождения: _____

Настоящим я свободно, своей волей и в своем интересе даю конкретное, предметное, информированное, однозначное и сознательное согласие на обработку АКЦИОНЕРНЫМ ОБЩЕСТВОМ «АЛЬФА-БАНК» (г. Москва, ул. Каланчевская, д. 27) (далее также – «Банк») следующей информации, относящейся к моим персональным данным, содержащейся в настоящем Заявлении, а также предоставленной мной Банку: фамилия, имя, отчество, СНИЛС, ИНН, контактные данные (мобильный телефон, адрес электронной почты), паспортные данные (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации), место работы, должность.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без использования таких средств, а также путем смешанной обработки персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (предоставление, доступ), блокирование, удаление, уничтожение) в целях исполнения обязательств Удостоверяющего центра АО «АЛЬФА-БАНК» по изготовлению невалифицированных сертификатов ключей проверки электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Выражаю согласие на внесение указанных в настоящем заявлении данных в реестр сертификатов, обязанность по ведению которого возложена на Удостоверяющий центр согласно ст. 13 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи». Я проинформирован и даю согласие на предоставление АО «АЛЬФА-БАНК» любому лицу по его обращению информации, содержащейся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи, во исполнение обязанности, возложенной на удостоверяющий центр п. 3 ч. 2 ст. 13 указанного Федерального закона.

Настоящее согласие на обработку персональных данных вступает в силу со дня его подписания и действует до достижения целей обработки персональных данных либо до отзыва настоящего согласия. Обработка персональных данных осуществляется в течении срока действия настоящего согласия. После истечения срока действия согласия удостоверяющий центр АО «АЛЬФА-БАНК» вправе осуществлять обработку персональных данных в случаях, предусмотренных действующим законодательством.

Согласие может быть отозвано по письменному заявлению в бумажном виде при личном прибытии Заявителя, при удовлетворении которого впоследствии УЦ аннулируются все выпущенные сертификаты данного Заявителя, при этом УЦ вправе не прекращать обработку персональных данных при наличии иных правовых оснований для продолжения обработки.

Даю согласие на создание сертификата ключа проверки электронной подписи в соответствии со сведениями, указанными в настоящем заявлении. Достоверность данных сведений подтверждаю.

Я проинформирован, что с момента подписания настоящего заявления присоединяюсь к Регламенту удостоверяющего центра АО «АЛЬФА-БАНК».

С настоящим Регламентом и приложениями к нему ознакомлен, полностью и безоговорочно соглашаюсь со всеми его условиями и обязуюсь соблюдать все положения указанного документа.

(Уполномоченный представитель
Заявителя)

(подпись)

(фамилия, инициалы)

(Должность руководителя)

(подпись)

(фамилия, инициалы)

« ____ » _____ 20 ____ года

* - обязательны для заполнения и включения в Сертификат поля, содержащие: ФИО владельца сертификата – физического лица, один из идентификаторов (ИНН, СНИЛС), наименование и адрес владельца сертификата – юридического лица.

Приложение №2в

к Регламенту Удостоверяющего центра АО «АЛЬФА-БАНК»

Форма заявления на создание и выдачу Обезличенного сертификата (для Банка)

Заявление на изготовление неквалифицированного сертификата ключа проверки электронной подписи

_____ (полное наименование юридического лица, включая организационно-правовую форму)

в лице _____

_____ (должность уполномоченного лица, фамилия, имя, отчество в родительном падеже)

действующего на основании _____

_____ (реквизиты распоряжения)

просит создать сертификат ключа проверки электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе в соответствии с указанными в настоящем заявлении данными:

Сокращенное наименование ЮЛ			
ИНН / КПП / ОГРН			
Страна / Область	РФ		
Населенный пункт			
Улица, номер дома, корпус, офис			
Адрес электронной почты			

Я, _____

_____ (фамилия, имя, отчество уполномоченного представителя Заявителя)

паспорт: серия _____ № _____ код подразделения _____ дата выдачи _____ г.

_____ (наименование органа, выдавшего документ)

дата рождения: _____ г., место рождения: _____

Настоящим я свободно, своей волей и в своем интересе даю конкретное, предметное, информированное, однозначное и сознательное согласие на обработку АКЦИОНЕРНЫМ ОБЩЕСТВОМ «АЛЬФА-БАНК» (г. Москва, ул. Каланчевская, д. 27) (далее также – «Банк») следующей информации, относящейся к моим персональным данным, содержащейся в настоящем Заявлении, а также предоставленной мной Банку: фамилия, имя, отчество, контактные данные (мобильный телефон, адрес электронной почты), паспортные данные (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации), место работы, должность.

Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без использования таких средств, а также путем смешанной обработки персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (предоставление, доступ), блокирование, удаление, уничтожение) в целях исполнения обязательств Удостоверяющего центра АО «АЛЬФА-БАНК» по изготовлению неквалифицированных сертификатов ключей проверки электронной подписи в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Выражаю согласие на внесение указанных в настоящем заявлении данных в реестр сертификатов, обязанность по ведению которого возложена на Удостоверяющий центр согласно ст. 13 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи». Я проинформирован и даю согласие на предоставление АО «АЛЬФА-БАНК» любому лицу по его обращению информации, содержащейся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи, во исполнение обязанности, возложенной на удостоверяющий центр п. 3 ч. 2 ст. 13 указанного Федерального закона.

Настоящее согласие на обработку персональных данных вступает в силу со дня его подписания и действует до достижения целей обработки персональных данных либо до отзыва настоящего согласия. Обработка персональных данных осуществляется в течении срока действия настоящего согласия. После истечения срока действия согласия удостоверяющий центр АО «АЛЬФА-БАНК» вправе осуществлять обработку персональных данных в случаях, предусмотренных действующим законодательством.

Согласие может быть отозвано по письменному заявлению в бумажном виде при личном прибытии Заявителя, при удовлетворении которого впоследствии УЦ аннулируются все выпущенные сертификаты данного Заявителя, при этом УЦ вправе не прекращать обработку персональных данных при наличии иных правовых оснований для продолжения обработки.

Даю согласие на создание сертификата ключа проверки электронной подписи в соответствии со сведениями, указанными в настоящем заявлении. Достоверность данных сведений подтверждаю.

Я проинформирован, что с момента подписания настоящего заявления присоединяюсь к Регламенту удостоверяющего центра АО «АЛЬФА-БАНК».

С настоящим Регламентом и приложениями к нему ознакомлен, полностью и безоговорочно соглашаюсь со всеми его условиями и обязуюсь соблюдать все положения указанного документа.

(Уполномоченный представитель
Заявителя)

(подпись)

(фамилия, инициалы)

« _____ » _____ 20 _____ года

Приложение №2г
к Регламенту Удостоверяющего центра АО «АЛЬФА-БАНК»
Форма доверенности

Доверенность № _____

Город _____, _____ 20 ____ года
(дата выдачи доверенности прописью)

(полное наименование юридического лица, включая организационно-правовую форму)

в лице _____

(должность, фамилия, имя, отчество руководителя юридического лица)

действующего на основании _____

(основание полномочий)

уполномочивает _____

(фамилия, имя, отчество Пользователя Удостоверяющего центра)

паспорт серии _____ № _____ выдан « ____ » _____ 20 ____ года

(наименование органа, выдавшего документ)

действовать от имени _____

(наименование юридического лица, включая организационно-правовую форму)

при использовании электронной подписи электронных документов, выступать в роли Пользователя Удостоверяющего центра и осуществлять действия в рамках Регламента Удостоверяющего центра АО «АЛЬФА-БАНК».

Уполномоченный представитель Заявителя наделяется правом подписать и получить все необходимые документы, подтверждающие факт оказания услуги по созданию сертификата ключа проверки электронной подписи.

Настоящая доверенность выдана без права передоверия и действительна по

« ____ » _____ 20 ____ года

Подпись Уполномоченного представителя
подтверждаю.

(подпись)

(фамилия, инициалы)

(Должность руководителя юридического лица)

(подпись)

(фамилия, инициалы)

« ____ » _____ 20 ____ года

М.П.

Приложение № 2д
к Регламенту Удостоверяющего центра АО «АЛЬФА-БАНК»
Форма заявления на прекращение действия Сертификата

**Заявление на прекращение действия неквалифицированного сертификата ключа
проверки электронной подписи**

Я,

_____ (фамилия, имя, отчество)

паспорт

серия _____ номер _____ выдан _____

_____ дата выдачи ____ / ____ / ____

Г.,

прошу прекратить действие сертификата ключа проверки электронной подписи в соответствии с указанными данными:

Фамилия, Имя, Отчество *			
Должность *			
СНИЛС *			
ИНН ФЛ *			
Сокращенное наименование ЮЛ			
ИНН / КПП / ОГРН			
Страна / Область	РФ		
Населенный пункт			
Улица, номер дома, корпус, офис\квартира (если имеется)			
Адрес электронной почты			

в связи с _____.

Владелец сертификата

(подпись)

(фамилия, инициалы)

Дата подачи заявления: « ____ » _____ 20 ____ г.

* - для Обезличенного сертификата указанные поля не заполняются

1. Регистрация пользователей.

Система регистрирует пользователя в УЦ на основании данных, содержащихся в сформированной пользователем заявке на портале Модуля управления ключами и сертификатами (далее – Модуль УКС).

Оператор УЦ осуществляет проверку соответствия сведений в заявке на создание и выдачу Сертификата с приложенными документами, проверяет наличие полномочий на сбор биометрических образцов у пользователя, производит идентификацию путем установления его личности по оригиналу основного документа, устанавливающим личность пользователя.

2. Генерация ключевой пары.

Генерация ключевой пары производится после идентификации пользователя оператором УЦ.

Для формирования ключа электронной подписи, ключа проверки электронной подписи, запроса на изготовление сертификата используются данные из поданной заявки на портале Модуля УКС.

Генерация ключевой пары и запроса на изготовления сертификата производится в программно-аппаратном комплексе Vipnet PKI Service, размещенном на стороне Банка.

3. Изготовление и выдача Сертификата Пользователю.

Сформированный в Vipnet Pki Service запрос на изготовление сертификата передается в систему Модуль УКС, которая в свою очередь передает его УЦ.

УЦ осуществляет изготовление сертификата в виде электронного документа в соответствии с поступившим запросом.

После изготовления сертификата УЦ направляет сформированный электронный документ в систему Модуль УКС, которая передает сертификат в Программно-аппаратный комплекс Vipnet PKI Service, размещенный на стороне Банка.

Пользователь системы распечатывает бланк на бумажном носителе, заверяет надлежащим образом и передает оператору УЦ.

Оператор УЦ заверяет надлежащим образом полученный бланк на бумажном носителе, сканирует и загружает в систему Модуль УКС.

Факт получения и согласия с содержанием полученного сертификата подтверждается пользователем подписью в бланке.

Срок изготовления сертификата не превышает 3 рабочих дней с момента поступления электронного запроса на изготовление сертификата в УЦ.

Процесс плановой смены ключей ЭП идентичен процессу первичного получения.

4. Состав и порядок хранения документов.

Для формирования сертификата пользователь предоставляет в Банк следующие документы:

- скан-копию основного документа, подтверждающего личность;
- скан-копию страхового номера индивидуального лицевого счета (СНИЛС);
- результаты тестирования в рамках пройденного курса «Электронная подпись: понятие, виды и порядок использования» (только работникам Банка);
- заявление на создание и выдачу сертификата.

Предоставленные документы, а также подписанный пользователем и оператором УЦ бланк хранятся в электронном виде и признаются равнозначными документам на бумажном носителе.

5. Аннулирование сертификата ключа проверки электронной подписи.

Для осуществления аннулирования (отзыва) сертификата пользователь передает заявление на аннулирование (отзыв) Оператору УЦ в виде бумажного документа.

Заявление на аннулирование (отзыв) сертификата должно содержать следующую информацию:

- ФИО владельца сертификата;
- Название организации;
- Серийный номер отзываемого сертификата;
- Название Бизнес-системы;
- Причину аннулирования (отзыва).

6. Структура сертификата ключа проверки электронной подписи пользователя

Название	Описание	Содержание
Базовые поля сертификата ключа проверки электронной подписи		
Validity Period	Срок действия сертификата (не может превышать 15 лет)	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = Организация владельца сертификата ключа проверки электронной подписи O = Организация владельца сертификата ключа проверки электронной подписи S = Субъект Российской Федерации места нахождения Организации владельца сертификата ключа проверки электронной подписи INN = ИНН физического лица владельца сертификата ключа проверки электронной подписи SNILS = СНИЛС владельца сертификата ключа проверки электронной подписи STREET = Улица места нахождения Организации владельца сертификата ключа проверки электронной подписи G = Имя и Отчество (при наличии) владельца сертификата ключа проверки электронной подписи SN = Фамилия владельца сертификата ключа проверки электронной подписи E = Электронная почта владельца сертификата ключа проверки электронной подписи INNLE – ИНН Организации владельца сертификата ключа проверки электронной подписи T = Должность владельца сертификата ключа проверки электронной подписи
Дополнения сертификата ключа проверки электронной подписи		
Certificate Template Information	Сведения о шаблоне сертификата	Шаблон=1.2.643.2.2.50.1.9.9617945.13916985.9654098.8989 965.6946.36015 Основная версия=1 Вспомогательная версия=0
Extended Key Usage	Улучшенный ключ 2.5.29.37	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Биометрия. Пользователь (1.3.6.1.4.1.16745.10.1)
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость, Цифровая подпись, Шифрование ключей, Шифрование данных

1. Генерация ключевой пары.

Генерация ключевой пары производится Заявителем с использованием СКЗИ, поддерживающим алгоритм электронной подписи ГОСТ 34.10-2012.

При создании ключевой пары создается файл запроса на создание и выдачу Сертификата безопасности в формате PKCS#10 (*.p10), который в последующем передается в УЦ.

2. Передача Заявителем регистрационных данных в УЦ.

Регистрация Заявителя УЦ происходит способами, предусмотренными ВНД Банка.

В составе регистрационных данных Заявитель передает Оператору УЦ следующие документы и сведения:

- файл запроса формата PKCS#10 на создание и выдачу Сертификата безопасности
- идентификатор системы, для которой предназначен Сертификат безопасности
- доменные имена системы
- документ или ссылку на согласованное архитектурное решение

Оператор УЦ осуществляет проверку соответствия сведений, предоставленных Заявителем в составе регистрационных данных, проводит идентификацию Заявителя.

3. Изготовление и выдача Сертификата безопасности Пользователю.

УЦ осуществляет изготовление Сертификата безопасности в виде электронного документа в соответствии с поступившим запросом на создание и выдачу Сертификата безопасности.

Оператор УЦ передает Сертификат безопасности Пользователю УЦ любым удобным способом.

Срок изготовления Сертификата безопасности не превышает 3 рабочих дней с момента поступления электронного запроса на создание и выдачу Сертификата безопасности в УЦ.

Процесс плановой смены ключей ЭП идентичен процессу первичного получения.

4. Аннулирование Сертификата безопасности ключа проверки электронной подписи.

Для осуществления аннулирования (отзыва) Сертификата безопасности пользователь сообщает Оператору УЦ о необходимости аннулирования (отзыва) с указанием следующей информации:

- Название организации;
- Серийный номер отзываемого Сертификата безопасности;
- Название Бизнес-системы;
- Причину аннулирования (отзыва).

5. Структура Сертификата безопасности

Название	Описание	Содержание
Базовые поля Сертификата безопасности		
Validity Period	Срок действия сертификата (не может превышать 15 лет)	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец SSL-сертификата	CN = Доменное имя защищаемой системы O = Организация владельца Сертификата безопасности S = Субъект Российской Федерации места нахождения Организации владельца Сертификата безопасности

		L = Населенный пункт местонахождения организации - Владельца Сертификата безопасности STREET = Улица места нахождения Организации владельца Сертификата безопасности E = Электронная почта организации – владельца Сертификата безопасности INNLE = ИНН Организации владельца Сертификата безопасности
Дополнения Сертификата безопасности		
Certificate Template Information	Сведения о шаблоне сертификата	Шаблон= 1.2.643.2.2.46.0.3 Основная версия=1 Вспомогательная версия=0
Extended Key Usage	Улучшенный ключ 2.5.29.37	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Проверка подлинности сервера (1.3.6.1.5.5.7.3.1) Сертификат безопасности (1.3.6.1.4.1.16745.12)
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость, Цифровая подпись, Шифрование ключей, Шифрование данных
Subject Alternative Name	Дополнительное имя субъекта 2.5.29.17	DNS-имя= Доменное имя защищаемой системы DNS-имя= Дополнительное доменное имя ...

1. Генерация ключевой пары.

Генерация ключевой пары производится Заявителем с использованием СКЗИ, поддерживающим алгоритм электронной подписи ГОСТ 34.10-2012.

При создании ключевой пары создается файл запроса на создание и выдачу Сертификата в формате PKCS#10 (*.p10), который в последующем передается в УЦ.

2. Передача Заявителем регистрационных данных в УЦ.

Регистрация Заявителя УЦ происходит способами, предусмотренными ВНД Банка.

В составе регистрационных данных Заявитель передает Оператору УЦ следующие документы и сведения:

- файл запроса формата PKCS#10 на создание и выдачу Сертификата;
- скан-копию подписанного по форме УЦ заявления на создание и выдачу Сертификата;
- скан-копию основного документа, удостоверяющего личность;
- данные о бизнес-системе Банка, в которой будет использоваться Сертификат;
- информацию о пройденном обучении по курсу «Электронная подпись: понятие, виды и порядок использования» (только работникам Банка);
- документ с полномочиями Заявителя УЦ действовать от имени юридического лица при обращении в УЦ за получением Сертификата.

Оператор УЦ осуществляет проверку соответствия сведений, предоставленных Заявителем в составе регистрационных данных, проводит идентификацию Заявителя в личном присутствии по оригиналу основного документа, удостоверяющего личность.

3. Изготовление и выдача Сертификата Пользователю.

Оператор УЦ отправляет в УЦ запрос на создание и выдачу Сертификата, переданный Оператору УЦ Заявителем в составе регистрационных данных.

УЦ осуществляет изготовление Сертификата в виде электронного документа в соответствии с поступившим запросом на создание и выдачу Сертификата.

После изготовления Сертификата УЦ направляет сформированный электронный документ в АРМ Оператора УЦ.

Оператор УЦ передает созданный в УЦ файл Сертификата Пользователю УЦ любым удобным способом.

Срок изготовления Сертификата не превышает 3 рабочих дней с момента поступления электронного запроса на создание и выдачу Сертификата в УЦ.

Процесс плановой смены ключей ЭП идентичен процессу первичного получения.

4. Аннулирование Сертификата.

Для осуществления аннулирования (отзыва) Сертификата пользователь передает заявление на аннулирование (отзыв) Оператору УЦ в виде бумажного документа.

Заявление на аннулирование (отзыв) Сертификата должно содержать следующую информацию:

- Название организации;
- ИНН организации
- Серийный номер отзываемого Сертификата;
- Фамилия имя отчество Владельца сертификата
- ИНН владельца сертификата
- СНИЛС владельца сертификата
- Причину аннулирования (отзыва).

1. Структура Сертификата

Название	Описание	Содержание
Базовые поля сертификата ключа проверки электронной подписи		
Validity Period	Срок действия сертификата (не может превышать 15 лет)	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = Наименование организации – Владельца O = Наименование организации – Владельца INNLE = ИНН организации - Владельца S = Субъект Российской Федерации места нахождения организации - Владельца L = Населенный пункт местонахождения организации - Владельца STREET = Улица места нахождения организации – Владельца SN = Фамилия Владельца Сертификата G = Имя и Отчество (при наличии) Владельца INN = ИНН физического лица Владельца SNILS = СНИЛС Владельца T = Должность работника организации – Владельца E = Электронная почта работника организации – Владельца
Дополнения Сертификата		
Certificate Template Information	Сведения о шаблоне сертификата	Шаблон=1.2.643.2.2.50.1.9.9617945.13916985.9654098.8989965.6946.36015 Основная версия=1 Вспомогательная версия=0
Extended Key Usage	Улучшенный ключ 2.5.29.37	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Универсальная система (1.3.6.1.4.1.16745.11)
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость, Цифровая подпись, Шифрование ключей, Шифрование данных