Утверждено Протоколом
Правления КИВИ Банк (АО)
№ 19 от «27» апреля 2015 года

Регламент предоставления услуг оператора удостоверяющего центра

ООО «КРИПТО-ПРО»

г. Москва, 2015 г.

1. Сведения об Операторе Удостоверяющего центра

КИВИ Банк (АО), именуемое в дельнейшем «Оператор Удостоверяющего центра» («Оператор»), зарегистрирован на территории Российской Федерации. Свидетельство о регистрации №2241 от 21 января 1993 года, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1027739328440 (Межрайонная инспекция МНС России №39 по г. Москве, 07 октября 2002 года, серия бланка 77 №007303852).
Реквизиты КИВИ Банк (АО):
Полное наименование: КИВИ Банк (акционерное общество)
Сокращенное наименование: КИВИ Банк (АО)
Юридический адрес: 123001, г. Москва, ул. Спиридоновка, д. 4 стр. 2.
Фактический адрес: 123001, г. Москва, ул. Спиридоновка, д. 4 стр. 2.
Адрес для корреспонденции: 123001, г. Москва, ул. Спиридоновка, д. 4 стр. 2.

Лицензии выданные ФСБ:

1. Лицензия № 13842Н от 06.10.2014 на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

РЕКВИЗИТЫ ДЛЯ РАСЧЕТОВ В РОССИЙСКИХ РУБЛЯХ:

Местонахождение: 123001, г. Москва, ул. Спиридоновка, д. 4 стр. 2
Тел.: +7 (495) 231-36-45, +7 (495) 231-36-46
Факс: +7 (495) 231-36-47
Корр. счет 30101810200000000416
В **Отделении 2 Москва**
БИК 044585416
ИНН/КПП 3123011520/775001001
ОКПО 22316525
ОКОНХ 96120, ОКВЭД 65.12
ОГРН 1027739328440, дата внесения записи «07» октября 2002г.

Контактные телефоны, факс, адрес электронной почты:
Тел.:
+7 (495) 231-36-45
+7 (495) 231-36-46
8-800-555-000-5 (звонок по России бесплатный)
Факс:
+7 (495) 231-36-47
E-mail:
bankinfo@qiwi.ru

2. Сведения об Удостоверяющем центре

Удостоверяющим центром, осуществляющим функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законодательством, является Общество с ограниченной ответственностью «КРИПТО-ПРО».
ООО «КРИПТО-ПРО» в качестве профессионального участника рынка услуг по созданию и выдаче сертификатов ключей подписей осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

1. Лицензия Центра ФСБ России по лицензированию, сертификации и защите государственной тайны на право осуществления распространения шифровальных (криптографических) средств;

2. Лицензия Центра ФСБ России по лицензированию, сертификации и защите государственной тайны на право осуществления технического обслуживания шифровальных (криптографических) средств;

3. Лицензия Центра ФСБ России по лицензированию, сертификации и защите государственной тайны на право предоставления услуг в области шифрования информации.

Сертификаты ключей подписей уполномоченного лица Удостоверяющего центра зарегистрированы Уполномоченным федеральным органом исполнительной власти Российской Федерации в части применения электронной подписи в Едином государственном реестре сертификатов уполномоченных лиц удостоверяющих центров.

3. Термины и определения

Электронный документ – документ, информация в котором представлена в электронной форме.
Средство электронной подписи – средство криптографической защиты информации (СКЗИ) «КриптоПро CSP», обеспечивающее реализацию следующих функций - создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи в электронном документе, создание закрытых и открытых ключей электронных подписей.
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;
Закрытый ключ электронной подписи - уникальная последовательность символов, известная владельцу сертификата открытого ключа подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.
Закрытый ключ электронной подписи признается действительным на определенный момент времени (действующий закрытый ключ) если:

- наступил момент времени начала действия закрытого ключа;
- срок действия закрытого ключа не истек;
- сертификат открытого ключа подписи, соответствующий данному закрытому ключу не аннулирован (отозван) и действие его не приостановлено.

Открытый ключ электронной подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.
Сертификат открытого ключа подписи (сертификат открытого ключа, сертификат ключа подписи) - электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, структура которого определяется настоящим Регламентом и который изготавливается Удостоверяющим центром для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа подписи.
Сертификат открытого ключа подписи действует на определенный момент времени (действующий сертификат) если:

- наступил момент времени начала действия сертификата открытого ключа;
- срок действия сертификата открытого ключа не истек;
- сертификат открытого ключа не аннулирован (отозван) и действие его не приостановлено.

Копия сертификата ключа подписи – документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный собственноручной подписью ответственного лица Оператора Удостоверяющего центра и печатью Оператора Удостоверяющего центра.
Список отозванных сертификатов (СОС) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.
Владелец сертификата ключа подписи – лицо, которому в установленном законом порядке выдан сертификат ключа проверки электронной подписи.
Псевдоним владельца сертификата ключа подписи – вымышленное имя лица, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре

Удостоверяющий центр – ООО «КРИПТО-ПРО», осуществляющее выполнение целевых функций Удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Оператор Удостоверяющего центра (Оператор) – КИВИ Банк (АО), наделенный Удостоверяющим центром полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей подписи Пользователей Удостоверяющего центра – полномочных представителей Стороны, присоединившейся к Регламенту.

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

- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление сертификата ключа подписи;
- реестр заявлений на аннулирование (отзыв) сертификата ключа подписи;
- реестр заявлений на приостановление/возобновление действия сертификата ключа подписи;
- реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;
- реестр заявлений на подтверждение электронной подписи уполномоченного лица Удостоверяющего центра в изданных сертификатах;
- реестр сертификатов ключей подписи;
- реестр изготовленных списков отозванных сертификатов;

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов открытого ключа подписи и списков отозванных сертификатов.

Пользователь Удостоверяющего центра (Пользователь УЦ) – лицо, зарегистрированное в Удостоверяющем центре и являющееся полномочным представителем Стороны, присоединившейся к Регламенту.

Информационная система - информационной система, в которой используются закрытые ключи ЭП и сертификаты открытых ключей ЭП, выданные Удостоверяющим центром, для формирования ЭП в электронных документах, обрабатывающихся в этой системе.

Рабочий день Оператора Удостоверяющего центра (далее – рабочий день) – промежуток времени с 9:30 по 18:30 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

Служба актуальных статусов сертификатов – сервис Удостоверяющего центра, обеспечивающий информирование пользователей о статусе сертификатов ключей подписей по протоколу OCSP (Online Certificate Status Protocol).

Служба штампов времени – сервис Удостоверяющего центра, обеспечивающий предоставление Пользователям Удостоверяющего центра штампов времени по протоколу TSP (Time-Stamp Protocol).

Штамп времени электронного документа (штамп времени) – электронный документ, подписанный электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

Cryptographic Message Syntax (CMS) – стандарт криптографических сообщений, описанный в RFC 3852 и RFC 3369. Удостоверяющий центр использует в своей работе криптографические сообщения, соответствующие данному стандарту с учетом RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

Online Certificate Status Protocol (OCSP) – протокол установления статуса сертификата открытого ключа, реализующий RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий Центр осуществляют свою работу в

соответствии со следующим стандартом PKCS - PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа.

Time-Stamp Protocol (TSP) – протокол получения штампа времени, реализующий RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

4. Общие положения

4.1. Статус Регламента

4.1.1. Настоящий Регламент предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (далее – «Регламент») определяет условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Сторон, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра и является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

4.1.2. Сторонами Регламента (далее – «Стороны») являются КИВИ Банк (АО), выступающее Оператором Удостоверяющего центра, и юридическое лицо, заключившее с Банком договор, предусматривающий обмен документами в электронной форме с использованием сертификатов ключа подписи, выданных удостоверяющим центром ООО «КРИПТО-ПРО», присоединившееся к Регламенту.

4.1.3. Любое заинтересованное лицо может ознакомиться с Регламентом в офисе Оператора Удостоверяющего центра по адресу: 123001, г. Москва, ул. Спиридоновка, д. 4 стр. 2, либо в Дополнительном офисе Банка, расположенном по адресу: 117648, г. Москва, мкр. Чертаново Северное, д. 1А, корп. 1, а также на web-сайте Банка в сети Интернет: http://www.bank.qiwi.ru.

4.2. Присоединение к Регламенту

4.2.1. Присоединение к Регламенту осуществляется путем подписания и предоставления Оператору Удостоверяющего центра Заявления к Регламенту по форме Приложения № 1 к настоящему Регламента.

4.2.2. Факт присоединения лица к Регламенту является полным принятием условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Подписного листа.

4.2.3. После присоединения к Регламенту в установленном порядке Стороны вступают в соответствующие договорные отношения на неопределённый срок.

4.2.4. Каждая из Сторон вправе без обращения в суд расторгнуть вышеуказанный договор, письменно уведомив другую сторону за 15 (пятнадцать) дней до дня расторжения. При этом Стороны в течение срока предупреждения до дня прекращения действия Регламента обязаны разрешить между собой все денежные и иные имущественные вопросы, связанные с настоящим Регламентом.

4.2.5. Прекращение действия Регламента не освобождает стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

4.3. Применение Регламента

4.3.1. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

4.3.2. В случае противоречия и/или расхождения названия какого-либо раздела Регламента со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

4.3.3. В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Регламенту с положениями собственно Регламента, Стороны считают доминирующим смысл и формулировки Регламента.

4.4. Изменение (дополнение) Регламента

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

4.4.2. Уведомление присоединившейся стороны о внесении изменений (дополнений) в Регламент осуществляется Оператором направлением по электронной почте в адрес уполномоченного представителя присоединившейся стороны – Пользователя Удостоверяющего центра - соответствующего информационного сообщения, а также размещением новой версии Регламента на web-сайте Банка в сети Интернет: http://www.bank.qiwi.ru.

4.4.3. Все изменения (дополнения), вносимые Оператором в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными для присоединившейся стороны по истечении 30 (тридцати) календарных дней с даты уведомления присоединившейся стороны о внесении указанных изменений (дополнений).

4.4.4. Все изменения (дополнения), вносимые Оператором в Регламент в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных нормативно-правовых актах.

4.4.5. 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. В случае несогласия с изменениями (дополнениями) пользователь Удостоверяющего центра имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренном п. 4.2.4. настоящего Регламента.

4.4.6. Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

5. Предоставление информации

5.1. Оператор вправе запросить у Стороны, присоединившейся к Регламенту, а присоединившаяся Сторона обязана предоставить Оператору документы, подтверждающие следующую информацию:

5.1.1. наименование Организации и основной государственный регистрационный номер, идентификационный номер налогоплательщика; нотариально заверенную копию Устава организации;

5.1.2. нотариально заверенную копию учредительного договора (если есть);

5.1.3. нотариально заверенную копию свидетельства ФНС о государственной регистрации;

5.1.4. копии протоколов, либо иных документов, о назначении уполномоченных лиц организации (в соответствии с учредительными документами организации) и/или надлежащим образом оформленные доверенности;

5.1.5. Сведения, необходимые для идентификации полномочного представителя Стороны, присоединившейся к Регламенту: фамилия, имя, отчество, номер паспорта, дата и кем выдан, место регистрации.

6. Права и обязанности сторон

6.1. Оператор обязан:

6.1.1. Предоставить Пользователю Удостоверяющего центра сертификат уполномоченного лица Удостоверяющего центра.

6.1.2. Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным в настоящем Регламенте.

6.1.3. Занести регистрационную информацию Пользователей Удостоверяющего центра в Реестр Удостоверяющего центра.

6.1.4. Обеспечить изготовление сертификата ключа подписи зарегистрированного в Удостоверяющем центре лица по заявлениям на изготовление сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте.

6.1.5. Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра по заявлению на аннулирование (отзыв) сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте.

6.1.6. Приостановить действие сертификата ключа подписи Пользователя Удостоверяющего центра по заявлению на приостановление действия сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте.

6.1.7. Возобновить действие сертификата ключа подписи Пользователя Удостоверяющего центра по заявлению на возобновление действия сертификата ключа подписи (исключительно в случае поступления заявления в период срока, на который действие сертификата было приостановлено), в соответствии с порядком, определенным в настоящем Регламенте.

6.2. Сторона, присоединившаяся к Регламенту, обязана:

6.2.1. Известить Удостоверяющий центр об изменениях в наименовании Организации, государственного регистрационного номера, идентификационного номера налогоплательщика и по требованию Удостоверяющего центра предоставить документы, указанные в п.5.1 настоящего Регламента, в течение 5 (пяти) рабочих дней с момента регистрации соответствующих изменений.

6.2.2. Пользователь Удостоверяющего центра, являющийся полномочным представителем присоединившейся Стороны обязан:

6.2.2.1. Сформировать открытые и закрытые ключи подписи на своем рабочем месте только с использованием средства электронной подписи и программного обеспечения, предоставляемого Удостоверяющим центром.

6.2.2.2. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

6.2.2.3. Применять для формирования электронной подписи только действующий личный закрытый ключ.

6.2.2.4. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

6.2.2.5. Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате ключа подписи (поля Key Usage, Extended Key Usage сертификата ключа подписи).

6.2.2.6. Немедленно обратиться к Оператору с заявлением на приостановление действия сертификата ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а также в случае если Пользователю Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами.

6.2.2.7. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на аннулирование (отзыв) которого подано на рассмотрение Оператором, в

течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата по момент времени официального уведомления об аннулировании (отзыве) сертификата.

6.2.2.8. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на приостановление действия которого подано на рассмотрение Оператором, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата по момент времени официального уведомления о приостановлении действия сертификата.

6.2.2.9. Не использовать личный закрытый ключ до предоставления Оператору подписанной копии сертификата ключа подписи, соответствующего данному закрытому ключу.

6.2.2.10.Своевременно, но не реже 1 раза в год, в порядке, определенном настоящим Регламентом, производить смену закрытого ключа электронной подписи Уполномоченного лица Присоединившейся Стороны.

6.3. Оператор имеет право:

6.3.1. Отказать в регистрации в Удостоверяющем центре уполномоченному представителю Стороны, присоединившейся к Регламенту, в случае ненадлежащего оформления необходимых регистрационных документов.

6.3.2. Отказать в изготовлении сертификата ключа подписи пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на изготовление сертификата ключа подписи, в том числе в случае сомнений в подлинности подписи Уполномоченного лица и/или Руководителя организации – присоединившейся стороны Регламента.

6.3.3. Отказать в аннулировании (отзыве) сертификата ключа подписи пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на аннулирование (отзыв) сертификата ключа подписи.

6.3.4. Отказать в приостановлении/возобновлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на приостановление/возобновление действия сертификата ключа подписи.

6.3.5. Отказать в аннулировании (отзыве) сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.3.6. Отказать в приостановлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.3.7. Отказать в возобновлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.3.8. В одностороннем порядке приостановить действие сертификата ключа подписи Пользователя Удостоверяющего центра с обязательным уведомлением владельца сертификата ключа подписи, действие которого приостановлено, и указанием обоснованных причин.

6.3.9. Отказать в изготовлении сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если использованное Пользователем Удостоверяющего центра для формирования запроса на сертификат ключа подписи средство криптографической защиты информации не поддерживается Удостоверяющим центром.

6.4. Сторона, присоединившаяся к Регламенту, имеет право:

6.4.1. Получить сертификат ключа подписи уполномоченного лица Удостоверяющего центра.

6.4.2. Получить список отозванных сертификатов ключей подписи, изготовленный Удостоверяющим центром.

6.4.3. Применять сертификат ключа подписи уполномоченного лица Удостоверяющего центра для проверки электронной подписи уполномоченного лица Удостоверяющего центра в сертификатах ключей подписи, изготовленных Удостоверяющим центром.

6.4.4. Применять список отозванных сертификатов ключей подписи, изготовленный Удостоверяющим центром, для проверки статуса сертификатов ключей подписи, изготовленных Удостоверяющим центром.

6.4.5. Применять сертификат ключа подписи Пользователя Удостоверяющего центра для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи.

6.4.6. Для хранения личного закрытого ключа применять любой носитель, поддерживаемый средством электронной подписи.

6.4.7. Обратиться к Оператору для аннулирования (отзыва) сертификата ключа подписи в течение срока действия соответствующего закрытого ключа.

6.4.8. Обратиться к Оператору для приостановления действия сертификата ключа подписи в течение срока действия соответствующего закрытого ключа.

6.4.9. Обратиться к Оператору для возобновления действия сертификата ключа подписи в течение срока действия соответствующего закрытого ключа и срока, на который действие сертификата было приостановлено.

7. Ответственность сторон

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

7.2. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

8. Разрешение споров

8.1. Сторонами в споре, в случае его возникновения, считаются Оператор и Сторона, присоединившаяся к Регламенту.

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

8.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их путем переговоров.

8.4. Спорные вопросы между Сторонами, неурегулированные путем переговоров, решаются в Арбитражном суде г. Москвы – для юридических лиц, и Чертановском районном суде города Москвы – для физических лиц.

9. Порядок предоставления и пользования услугами Удостоверяющего центра

9.1. Регистрация Пользователей Оператором Удостоверяющего центра

Оператор Удостоверяющего центра осуществляет регистрацию Пользователя в Удостоверяющем центре только в том случае, если Сторона, полномочным представителем которой является регистрирующееся лицо, присоединилась к настоящему Регламенту.

9.1.1. Регистрация пользователей и изготовление первого сертификата в централизованном режиме

Регистрация Пользователя в Удостоверяющем Центре осуществляется на основании заявления на регистрацию при личном прибытии лица, проходящего процедуру регистрации, в офис Оператора.

Форма заявления на регистрацию приведена в Приложении № 3 к настоящему Регламенту.

Регистрирующееся лицо должно предоставить доверенность, выданную на его имя Стороной, присоединившейся к Регламенту, на совершение действий в рамках настоящего Регламента по форме Приложения № 4 к настоящему Регламенту.

В случае если регистрирующееся лицо не может прибыть лично в офис Оператора, Сторона, присоединившаяся к Регламенту, должна выдать представителю, пребывающему в офис Оператора для регистрации, Доверенность на регистрацию соответствующего Пользователя. Форма Доверенности приведена в Приложении № 5 к настоящему Регламенту.

Ответственный сотрудник Оператора Удостоверяющего Центра выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по паспорту.

После положительной идентификации лица, проходящего процедуру регистрации, ответственный сотрудник Оператора Удостоверяющего Центра принимает документы и осуществляет их рассмотрение.

Заявление на регистрацию рассматривается ответственным сотрудником Оператора Удостоверяющего Центра в течение 1 (Один) часа с момента поступления.

В случае отказа в регистрации, заявление на регистрацию вместе с приложениями возвращается заявителю с отметкой ответственного сотрудника Оператора Удостоверяющего Центра.

При принятии положительного решения, ответственный сотрудник Оператора Удостоверяющего Центра выполняет регистрационные действия по занесению регистрационной информации в реестр Удостоверяющего Центра, изготавливает ключи подписи и сертификат ключа подписи на предоставляемый лицом, проходящим процедуру регистрации, ключевой носитель.

Ответственный сотрудник Оператора Удостоверяющего Центра изготавливает две копии сертификата ключа подписи на бумажном носителе по форме определенной Приложением № 11 к настоящему Регламенту. Все копии сертификата открытого ключа на бумажном носителе заверяются собственноручной подписью лица, проходящего процедуру регистрации, или собственноручной подписью доверенного лица, а также собственноручной подписью ответственного сотрудника Оператора Удостоверяющего Центра и печатью Оператора Удостоверяющего Центра.

По окончании процедуры регистрации Пользователю УЦ выдаются:

ключевой носитель, содержащий:

- закрытый и открытый ключ подписи, записанные в виде ключевого контейнера в формате, определяемом средством электронной подписи;

дополнительно Пользователю УЦ предоставляются (на съемном носителе информации):

- сертификат ключа подписи Пользователя УЦ в электронной форме в виде файла, соответствующий закрытому ключу;

- копию сертификата ключа подписи уполномоченного лица Удостоверяющего Центра в электронной форме в виде файла.
- копия сертификата ключа подписи Пользователя УЦ на бумажном носителе.

9.1.2. Регистрация пользователя и изготовление первого сертификата в распределенном режиме

Регистрация пользователя в распределенном режиме осуществляется на основании заявления на регистрацию по форме Приложения №3 к настоящему Регламенту. Заявление на регистрацию предоставляется Оператору Удостоверяющего центра посредством электронной почты, почтовой либо курьерской связи (без личного прибытия регистрирующегося лица). Дополнительно регистрирующееся лицо должно предоставить доверенность, выданную на его имя Стороной, присоединившейся к Регламенту, на совершение действий в рамках настоящего Регламента по форме Приложения № 4 к настоящему Регламенту.

После принятия положительного решения о регистрации Оператор Удостоверяющего центра предоставляет пользователю сертификат уполномоченного лица Удостоверяющего центра и актуальный список отозванных сертификатов в виде файлов на съемном носителе или по электронной почте, а также адрес web-страницы в сети Интернет регистрации в Удостоверяющем центре.

Пользователь производит установку и настройку своего рабочего места и с помощью автоматизированного рабочего места (далее – «АРМ») пользователя Удостоверяющего центра формирует и направляет запрос на регистрацию в электронной форме в Удостоверяющий центр.

Ответственное лицо Оператора Удостоверяющего центра производит сравнение идентификационной информации, указанной в заявлении на регистрацию с информацией содержащейся в запросе на регистрацию, поданном в электронной форме. В случае идентичности указанной идентификационной информации пользователь регистрируется Оператором в Удостоверяющем центре.

Регистрация пользователя и уведомление пользователя о регистрации должны быть осуществлены не позднее 3 (трех) рабочих дней следующих за рабочим днем, в течение которого был подан запрос на регистрацию в Удостоверяющий центр в электронном виде.

После получения уведомления о регистрации в Удостоверяющем центре пользователь с помощью АРМ пользователя Удостоверяющего центра генерирует пару ключей, формирует и направляет запрос на сертификат открытого ключа в электронной форме в Удостоверяющий центр и подает заявление на изготовление сертификата по форме Приложения № 7 к настоящему Регламенту (подача заявления осуществляется посредством электронной почты, почтовой либо курьерской связи).

Ответственное лицо Оператора Удостоверяющего центра производит сравнение идентификационной информации, указанной в заявлении на изготовление сертификата с информацией указанной в запросе на сертификат, поданном в электронной форме. В случае идентичности идентификационной информации ответственное лицо издает сертификат открытого ключа пользователя и распечатывает два экземпляра копии сертификата открытого ключа. Оба экземпляра визируются ответственным сотрудником Оператора Удостоверяющего центра, заверяются печатью Оператора Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются пользователю Удостоверяющего центра.

Изготовление сертификата и уведомление пользователя об изготовлении сертификата должны быть осуществлены не позднее 3 (трех) рабочих дней следующих за рабочим днем, в течение которого был подан запрос на изготовление сертификата в электронном виде.

После получения уведомления об изготовлении сертификата пользователь с помощью АРМ пользователя Удостоверяющего центра вводит секретную ключевую фразу, указанную при генерации ключевой пары, производит установку сертификата на своем рабочем месте и подтверждает ее.

До истечения 30 (тридцати) календарных дней с момента получения уведомления об изготовлении сертификата пользователь должен подписать и соответствующим образом заверить

два экземпляра сертификата открытого ключа и предоставить Оператору Удостоверяющего центра один экземпляр.
В случае предоставления документов посредством электронной почты, оригиналы документов необходимо передать Оператору Удостоверяющего центра в течении 30 (тридцати) дней с момента регистрации в Удостоверяющем центре. Если оригиналы документов не поступили в Удостоверяющий центр в течение 30 (тридцати) дней после регистрации, Оператор вправе приостановить действие сертификата в одностороннем порядке.

9.2. Изготовление и получение ключей подписи и сертификата ключа подписи

Изготовление ключей подписи и сертификата открытого ключа Пользователя УЦ осуществляется при плановой и внеплановой смене закрытого ключа подписи Пользователя УЦ.
Формирование ключей подписи и сертификата ключа подписи Пользователя УЦ осуществляется Оператором Удостоверяющего Центра на основании заявления на изготовление сертификата ключа подписи.
Заявление на изготовление сертификата ключа подписи может подаваться в Удостоверяющий центр в бумажной форме при личном прибытии Пользователя УЦ в офис Оператора Удостоверяющего Центра и в электронной форме с рабочего места Пользователя УЦ с использованием программного обеспечения, предоставляемого Удостоверяющим Центром.

9.2.1. Изготовление и получение сертификата ключа подписи по заявлению, поданному в бумажной форме

Форма заявления на изготовление ключей подписи и сертификата ключа подписи приведена в Приложении № 6 к настоящему Регламенту.
В том случае, если Пользователь УЦ не может прибыть лично в офис Оператора Удостоверяющего центра, Сторона, присоединившаяся к Регламенту должна выдать лицу, пребывающему в офис Оператора Удостоверяющего центра, Доверенность на получение ключей и сертификата ключа подписи соответствующего Пользователя УЦ. Форма Доверенности приведена в Приложении № 7 к настоящему Регламенту.
Ответственный сотрудник Оператора Удостоверяющего Центра выполняет процедуру идентификации Пользователя УЦ или доверенного лица путем установления личности по паспорту.
После положительной идентификации Пользователя УЦ или доверенного лица Ответственный сотрудник Оператора Удостоверяющего Центра принимает документы и осуществляет их рассмотрение.
Заявление на изготовление ключей подписи и сертификата открытого ключа рассматривается ответственным сотрудником Оператора Удостоверяющего Центра в течение 1 (одного) часа с момента поступления.
В случае отказа в изготовлении ключей подписи и сертификата открытого ключа, заявление на изготовление ключей подписи и сертификата открытого ключа вместе с приложениями возвращается заявителю с отметкой ответственного сотрудника Оператора Удостоверяющего Центра.
При принятии положительного решения, ответственный сотрудник Оператора Удостоверяющего Центра изготавливает ключи подписи и сертификат ключа подписи на предоставляемый Пользователем УЦ или его представителем ключевой носитель.
Ответственный сотрудник Оператора Удостоверяющего Центра изготавливает две копии сертификата ключа подписи на бумажном носителе по форме определенной Приложением № 11 к настоящему Регламенту. Все копии сертификата ключа подписи на бумажном носителе заверяются собственноручной подписью Пользователя УЦ, или собственноручной подписью доверенного лица, а также собственноручной подписью ответственного сотрудника Оператора Удостоверяющего Центра и печатью Оператора Удостоверяющего Центра.
По окончании процедуры изготовления ключей и сертификата ключа подписи Пользователю УЦ выдаются:

ключевой носитель, содержащий:

- закрытый и открытый ключ подписи, записанные в виде ключевого контейнера в формате, определяемом средством электронной подписи;

дополнительно Пользователю УЦ предоставляются:

- сертификат ключа подписи Пользователя УЦ в электронной форме в виде файла, соответствующий закрытому ключу;
- копию сертификата ключа подписи уполномоченного лица Удостоверяющего Центра в электронной форме в виде файла.
- копия сертификата ключа подписи Пользователя УЦ на бумажном носителе.

9.2.2. Изготовление и получение сертификата ключа подписи по заявлению, поданному в электронной форме

Подача Пользователем УЦ заявления на изготовление сертификата ключа подписи в электронной форме осуществляется с использованием программного обеспечения, предоставляемого Удостоверяющим Центром.

Заявление на изготовление сертификата ключа подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на сертификат ключа подписи в формате PKCS#10, а электронная подпись выполняется действующим закрытым ключом Пользователя УЦ.

Значения полей Subject, Key Usage, Extended Key Usage, содержащиеся в запросе на сертификат должны быть идентичны значениям этих полей в сертификате ключа подписи, соответствующего закрытому ключу Пользователя УЦ, которым сформирована электронная подпись в заявлении на изготовление сертификата ключа подписи Пользователя УЦ.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Оператора Удостоверяющего центра проверяет корректность электронной подписи заявления и устанавливает его автора, затем сравнивает значения полей Subject, Key Usage, Extended Key Usage, содержащиеся в запросе на сертификат, со значениями, указанными в сертификате ключа подписи автора настоящего заявления.

В случае отрицательного результата проведенных проверок, а также иных случаях, установленных настоящим Регламентом, ответственный сотрудник Оператора Удостоверяющего Центра отклоняет заявление на изготовление сертификата ключа подписи.

Срок рассмотрения заявления на изготовление сертификата ключа подписи составляет один рабочий день с момента регистрации заявления на изготовление сертификата ключа подписи в Удостоверяющем центре. В случае отказа в изготовлении сертификата ключа подписи ответственный сотрудник Оператора Удостоверяющего центра официально уведомляет Пользователя УЦ об этом в срок, установленный для рассмотрения заявления.

При принятии положительного решения, ответственный сотрудник Оператора Удостоверяющего Центра принимает заявление на изготовление сертификата ключа подписи и осуществляет изготовление сертификата ключа подписи.

Срок изготовления сертификата ключа подписи составляет 3 (Три) рабочих дня с момента регистрации заявления на сертификат ключа подписи в Удостоверяющем Центре. После изготовления сертификата ключа подписи Удостоверяющий центр официально уведомляет по электронной почте Пользователя УЦ об этом, после чего Пользователь УЦ устанавливает сертификат ключа подписи на своем рабочем месте с использованием предоставленного Удостоверяющим центром программного обеспечения.

Дополнительно ответственный сотрудник Оператора Удостоверяющего центра формирует и направляет Пользователю УЦ два экземпляра копии сертификата ключа подписи, подписанные ответственным сотрудником Оператора Удостоверяющего центра и заверенные печатью Оператора Удостоверяющего центра.

До истечения 30 (тридцати) календарных дней с момента официального уведомления пользователя об изготовлении сертификата ключа подписи Пользователь УЦ должен подписать

два экземпляра копии сертификата ключа подписи и предоставить Оператору Удостоверяющего центра один экземпляр.

9.3. Аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра

Для осуществления аннулирования (отзыва) сертификата ключа подписи Пользователь УЦ подает заявление на аннулирование (отзыв) сертификата ключа подписи Оператору Удостоверяющего Центра.

Заявление на аннулирование (отзыв) сертификата ключа подписи может подаваться в бумажной форме (при личном прибытии Пользователя УЦ в офис Оператора Удостоверяющего Центра, либо посредством почтовой или курьерской связи) и в электронной форме с рабочего места Пользователя УЦ с использованием программного обеспечения, предоставляемого Удостоверяющим Центром.

9.3.1. Аннулирование (отзыв) сертификата ключа подписи по заявлению, поданному в бумажной форме

Форма заявления на аннулирование (отзыв) сертификата ключа подписи приведена в Приложении № 8 к настоящему Регламенту.

Заявление на аннулирование (отзыв) сертификата ключа подписи заверяется собственноручной подписью владельца сертификата ключа подписи (Пользователя УЦ) и подается в офис Оператора Удостоверяющего Центра.

Подача заявления и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на аннулирование (отзыв) сертификата ключа подписи и официальное уведомление Пользователя УЦ об аннулировании (отзыве) сертификата ключа подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление Оператору Удостоверяющего Центра.

Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате. Временем аннулирования (отзыва) сертификата ключа подписи признается время издания списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.

9.3.2. Аннулирование (отзыв) сертификата ключа подписи по заявлению, поданному в электронной форме

Подача Пользователем УЦ заявления на аннулирование (отзыв) сертификата ключа подписи в электронной форме осуществляется с использованием программного обеспечения, предоставляемого Удостоверяющим Центром.

Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на запрос на отзыв сертификата ключа подписи, а электронная подпись выполняется действующим закрытым ключом Пользователя УЦ.

Запрос на отзыв сертификата ключа подписи представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер отзываемого сертификата ключа подписи;
- ReasonCode - код причины отзыва из следующего перечня допустимых значений:
  - "0" Не указана
  - "1" Компрометация ключа
  - "2" Компрометация ЦС

- "3" Изменение принадлежности
- "4" Сертификат заменен
- "5" Прекращение работы

- SomeComment - текстовое значение комментария владельца сертификата ключа подписи.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Оператора Удостоверяющего центра проверяет корректность электронной подписи заявления и устанавливает его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа подписи (отзываемого сертификата ключа подписи), серийный номер которого указан в запросе на отзыв сертификата ключа подписи.

В случае отрицательного результата проведенных проверок, а также иных случаях, установленных настоящим Регламентом, ответственный сотрудник Оператора Удостоверяющего Центра отклоняет заявление на аннулирование (отзыв) сертификата ключа подписи.

Срок рассмотрения заявления на аннулирование (отзыв) сертификата ключа подписи составляет 1 (один) рабочий день с момента регистрации заявления в Удостоверяющем центре. В случае отказа в аннулировании (отзыве) сертификата ключа подписи Оператор Удостоверяющего центра официально уведомляет Пользователя УЦ об этом в срок, установленный для рассмотрения заявления.

При принятии положительного решения, ответственный сотрудник Оператора Удостоверяющего Центра аннулирует (отзывает) сертификат ключа подписи.

Обработка заявления на аннулирование (отзыв) сертификата ключа подписи и официальное уведомление Пользователя УЦ об аннулировании (отзыве) сертификата ключа подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было зарегистрировано заявление в Удостоверяющем Центре.

Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате. Временем аннулирования (отзыва) сертификата ключа подписи признается время издания списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.

9.4. Приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра

Для осуществления приостановления действия сертификата ключа подписи Пользователь УЦ подает заявление на приостановление действия сертификата ключа подписи.

Приостановление действия сертификата ключа подписи Пользователя УЦ осуществляется Оператором Удостоверяющего центра на основании заявления, поступающего в устной, бумажной или электронной форме.

Заявление в устной форме делается в офис Оператора Удостоверяющего Центра по телефону.

Заявитель должен сообщить ответственному сотруднику Оператора Удостоверяющего Центра следующую информацию:

- Идентификационные данные владельца сертификата ключа подписи;
- серийный номер сертификата ключа подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключа подписи;
- ключевую фразу Пользователя УЦ (определяемой в процессе регистрации Пользователя УЦ).

Заявление принимается только в случае положительной аутентификации Пользователя УЦ (совпадения ключевой фразы переданной в заявлении с информацией из реестра пользователей Удостоверяющего Центра).

Заявление в бумажной форме подается в офис Оператора Удостоверяющего Центра по форме, определенной Приложением № 9 к настоящему Регламенту.

Заявление в бумажной форме содержит следующую информацию:

- Идентификационные данные владельца сертификата ключа подписи;
- серийный номер сертификата ключа подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключа подписи;
- дата и время подачи заявления.

Заявление на приостановление действия сертификата ключа подписи заверяется собственноручной подписью владельца сертификата (Пользователя УЦ) и подается в офис Оператора Удостоверяющего Центра (при личном прибытии заявителя, либо посредством почтовой или курьерской связи).

Заявление на приостановление действия сертификата ключа подписи в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на приостановление действия сертификата, а электронная подпись осуществляется действующим закрытым ключом Пользователя УЦ.

Запрос на приостановление действия сертификата представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, HD=HoldDuration, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер сертификата открытого ключа, действие которого требуется приостановить;
- ReasonCode – «6» – приостановление действия;
- HoldDuration – срок, на который приостанавливается действие сертификата, в следующем формате: Y-M-W-D-H-M, где:

Y – число лет;
M – число месяцев;
W – число недель;
D – число дней;
H – число часов;
M – число минут;

- SomeComment - текстовое значение комментария владельца сертификата ключа подписи.

Заявление на приостановление действия сертификата ключа подписи в электронном виде формируется и подается в Удостоверяющий Центр с использованием программного обеспечения, предоставляемого Удостоверяющим Центром.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Оператора Удостоверяющего центра проверяет корректность электронной подписи заявления и устанавливает его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа подписи (сертификата ключа подписи, действие которого требуется приостановить), серийный номер которого указан в запросе на приостановление действия сертификата ключа подписи.

Действие сертификата приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата составляет 10 (Десять) дней.

Подача заявления на приостановление действия сертификата в Удостоверяющий Центр и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на приостановление действия сертификата ключа подписи и оповещение Пользователя УЦ о приостановлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий Центр.
Официальным уведомлением о приостановлении действия сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено. Временем приостановления действия сертификата ключа подписи признается время издания списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, указанное в поле thisUpdate изданного списка отозванных сертификатов.
Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.
В том случае, если в течение срока приостановления действия сертификата ключа подписи Пользователя УЦ Оператору Удостоверяющего Центра не поступает заявление от Пользователя УЦ о возобновлении действия сертификата, сертификат аннулируется (отзывается) Удостоверяющим Центром.

9.5. Возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра
Для осуществления возобновления действия сертификата ключа подписи Пользователь УЦ подает заявление на возобновление действия сертификата.
Возобновление действия сертификата ключа подписи Пользователя УЦ осуществляется ответственным сотрудником Оператора Удостоверяющего Центра на основании заявления на возобновление действия сертификата ключа подписи, поступающего в бумажной или электронной форме.
Заявление в бумажной форме подается в офис Оператора Удостоверяющего Центра по форме, определенной Приложением № 10 к настоящему Регламенту.

Заявление в бумажной форме содержит следующую информацию:

- идентификационные данные владельца сертификата ключа подписи;
- серийный номер сертификата ключа подписи, действие которого требуется возобновить;
- дата и время подачи заявления.

Заявление на возобновление действия сертификата ключа подписи в бумажной форме заверяется собственноручной подписью владельца сертификата (Пользователя УЦ) и подается в офис Оператора Удостоверяющего Центра (при личном прибытии заявителя, либо посредством почтовой или курьерской связи).

Заявление на возобновление действия сертификата ключа подписи в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на возобновление действия сертификата, а электронная подпись осуществляется действующим закрытым ключом Пользователя УЦ.

Запрос на возобновление действия сертификата представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер сертификата ключа подписи, действие которого требуется возобновить;
- ReasonCode – «-1» - возобновление действия;
- SomeComment - текстовое значение комментария владельца сертификата ключа подписи.

Заявление на возобновление действия сертификата открытого ключа формируется и подается в электронном виде в Удостоверяющий Центр с использованием программного обеспечения, предоставляемого Удостоверяющим Центром.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Оператора Удостоверяющего центра проверяет корректность электронной подписи заявления и устанавливает его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа подписи (сертификата ключа подписи, действие которого требуется возобновить), серийный номер которого указан в запросе на возобновление действия сертификата ключа подписи.

Подача заявления на возобновление действия сертификата в Удостоверяющий Центр и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на возобновление действия сертификата и оповещение Пользователя УЦ о возобновлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий Центр.

Официальным уведомлением о возобновлении действия сертификата ключа подписи является опубликование списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено. Временем возобновления действия сертификата ключа подписи признается время издания списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.

9.6. Подтверждение подлинности ЭП в электронном документе

Для подтверждения подлинности ЭП в электронных документах, циркулирующих в Информационной системе, Пользователь УЦ подает Заявление на подтверждение подлинности ЭП в электронном документе в офис Оператора Удостоверяющего Центра.

Подтверждение подлинности ЭЦП электронного документа осуществляется на основании заявления, содержащего следующую информацию:

- Дата и время подачи заявления;
- Идентификационные данные Пользователя УЦ, ЭП которого требуется проверить в электронном документе;
- Серийный номер сертификата ключа подписи, на котором требуется проверить ЭП электронного документа;
- дата и время формирования ЭП в электронном документе.

Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является файл на сменном магнитном носителе, содержащий электронный документ.

Предоставляемый файл получается путем экспорта электронного документа, к которому применена электронная подпись, из Информационной системы.

Электронная подпись в предоставленном электронном документе признается равнозначной собственноручной подписи при выполнении следующих условий:

- сертификат ключа подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, не утратил силу (действует) на момент формирования ЭП в электронном документе - дата и время формирования ЭП в электронном документе, указанная в заявлении на подтверждение подлинности ЭП;
- электронная подпись, проверенная сертификатом ключа подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, верна;
- электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи – в поле Extended Key Usage;
- Формирование электронной подписи осуществлено без нарушений условий настоящего Регламента.

Срок проведения работ по заявлению на подтверждение подлинности ЭП в электронном документе и предоставлению заключения о произведенной проверке составляет 15 (Пятнадцать) рабочих дней с момента его предоставления Оператору Удостоверяющего центра.
Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Оператора Удостоверяющего Центра. При проведении указанных работ Оператор Удостоверяющего центра (комиссия) имеет право привлекать к проведению экспертных работ специалистов Удостоверяющего центра.
Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение в письменной форме, подписанное всеми членами комиссии и заверенное печатью Оператора Удостоверяющего Центра.

Заключение содержит:

- результат проверки ЭП электронного документа;
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные комиссии для проведения проверки;

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручными подписями всех членов комиссии.

9.7. Подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра в изданных сертификатах

Для подтверждения подлинности ЭП уполномоченного лица Удостоверяющего Центра в сертификате ключа подписи Пользователь УЦ подает заявление на подтверждение подлинности ЭП уполномоченного лица Удостоверяющего Центра в сертификате ключа подписи Оператору Удостоверяющего Центра.
Заявление должно содержать следующую информацию:

- Дата и время подачи заявления;
- Идентификационные данные субъекта, в сертификате ключа подписи которого необходимо подтвердить ЭП уполномоченного лица Удостоверяющего Центра;
- Серийный номер сертификата ключа подписи, в котором необходимо подтвердить ЭП уполномоченного лица Удостоверяющего Центра.

Обязательным приложением к заявлению на подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра в сертификате ключа подписи является сменный магнитный носитель, содержащий файл сертификата ключа подписи, подвергающегося процедуре проверки.
Срок проведения работ по подтверждению подлинности ЭП и предоставлению заключения о произведенной проверке составляет 15 (Пятнадцать) рабочих дней с момента его предоставления Оператору Удостоверяющего Центра.
На основании полученного заявления Оператор Удостоверяющего центра установленным порядком обращается в Удостоверяющий центр, который осуществляет подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра в сертификате ключа подписи.
Результатом проведения работ по подтверждению подлинности ЭП уполномоченного лица Удостоверяющего Центра в сертификате ключа подписи является заключение Удостоверяющего

Центра в письменной форме, подписанное уполномоченным лицом Удостоверяющего центра и заверенное печатью Удостоверяющего центра.

Заключение содержит:

- результат проверки ЭП уполномоченного лица Удостоверяющего Центра;
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные для проведения проверки;

Отчет по выполненной проверке составляется в простой письменной форме.

9.8. Прочие условия

9.8.1. Регистрация Пользователя может быть осуществлена уполномоченным представителем Пользователя Удостоверяющего центра, действующим на основании доверенности на осуществление регистрации в Удостоверяющем центре. Доверенность на осуществление регистрации в Удостоверяющем центре должна быть составлена и оформлена по форме Приложения № 5 к настоящему Регламенту.

9.8.2. Период времени действия закрытого ключа, соответствующего выданному сертификату ключа подписи Пользователя Удостоверяющего центра должен находиться в пределах периода времени, на который выдана Стороной, присоединившейся к Регламенту, соответствующая доверенность на совершение действий, определенных положениями настоящего Регламента для Пользователя Удостоверяющего центра.

10. Структура сертификатов ключей подписи и сроки действия ключевых документов

10.1. Структура сертификата ключа подписи уполномоченного лица Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SybjectType (Тип владельца сертификата) =ЦС Path Length Constraint (Ограничение на длину пути –ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих центров)= Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор версии сертификата	Версия сертификата Уполномоченного лица Удостоверяющего центра

10.2. Структура сертификата ключа подписи Пользователя Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество или псевдоним OrganizationUnit = Подразделение Organization = Организация Title = Должность Locality = Город State = Субъект Федерации Country = Страна = RU Email = Электронная почта Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата и Оператором Удостоверяющего центра. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре
Application Policy	Политика применения	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора закрытого ключа уполномоченного лица Удостоверяющего центра, с использованием которого издан сертификат и список отозванных сертификатов
Authority Information Access	Адрес Службы актуальных статусов сертификатов	URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280

10.3. Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CommonName = УЦ КРИПТО-ПРО – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица Удостоверяющего Центра

10.4. Расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа подписи содержат сведения об отношениях, при которых электронный документ будет иметь юридическое значение. Наличие в сертификате ключа подписи области

использования «Пользователь Центра Регистрации (1.2.643.2.2.34.6)» устанавливает, что владелец указанного сертификата имеет право подписывать электронной подписью электронные документы, определенные настоящим Регламентом для Пользователя Удостоверяющего центра.

10.5. Сроки действия ключевых документов

10.5.1. Срок действия закрытого ключа Уполномоченного лица Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности удостоверяющего центра, и для средства электронной подписи, с использованием которого данный закрытый ключ был сформирован.

Начало периода действия закрытого ключа уполномоченного лица Удостоверяющего центра исчисляется с даты и времени генерации закрытого ключа уполномоченного лица Удостоверяющего центра.

Срок действия сертификата ключа подписи Уполномоченного лица Удостоверяющего центра не превышает 30 (тридцать) лет. Время начала периода действия сертификата ключа подписи Уполномоченного лица Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

10.5.2. Срок действия закрытого ключа Пользователя Удостоверяющего составляет 1 (один) год.

Начало периода действия закрытого ключа Пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа подписи.

Срок действия сертификата ключа подписи Пользователя Удостоверяющего центра не превышает 30 (тридцать) лет. Время начала периода действия сертификата ключа подписи Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

11. Дополнительные положения

11.1. Плановая смена ключей уполномоченного лица Удостоверяющего центра

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) Уполномоченного лица Удостоверяющего центра выполняется в период действия закрытого ключа Уполномоченного лица Удостоверяющего центра.
Процедура плановой смены ключей уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего центра генерирует новый закрытый и соответствующий ему открытый ключ;
- Уполномоченное лицо Удостоверяющего центра изготавливает новый сертификат ключа подписи уполномоченного лица Удостоверяющего центра.

Старый закрытый ключ Уполномоченного лица Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого закрытого ключа Уполномоченного лица Удостоверяющего центра.
По истечении 1 (одного) года с момента проведения плановой смены ключей Уполномоченного лица Удостоверяющий центр изготавливает список отозванных сертификатов, соответствующий старому закрытому ключу, со сроком действия соответствующим сроку действия старого сертификата Уполномоченного лица Удостоверяющего центра (значение поля nextUpdate списка отозванных сертификатов совпадает со значением поля notAfter поля Validity сертификата ключа подписи Уполномоченного лица Удостоверяющего центра). Изданный список отозванных сертификатов публикуется Удостоверяющим центром, изготовление нового списка отозванных сертификатов, соответствующего старому закрытому ключу Уполномоченного лица Удостоверяющего центра, более не осуществляется.

11.2. Компрометация ключевых документов уполномоченного лица Удостоверяющего центра, внеплановая смена ключей уполномоченного лица Удостоверяющего центра

В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра сертификат Уполномоченного лица Удостоверяющего Центра аннулируется (отзывается), Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о компрометации на сайте Удостоверяющего центра. Все сертификаты, изданные с использованием скомпрометированного ключа Уполномоченного лица Удостоверяющего центра, считаются аннулированными.
После аннулирования сертификата Уполномоченного лица Удостоверяющего Центра выполняется процедура внеплановой смены ключей Уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключей Уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей Уполномоченного лица Удостоверяющего.
Все действовавшие на момент компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра сертификаты ключей подписей, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

11.3. Компрометация ключевых документов Пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа.

В случае компрометации или угрозы компрометации закрытого ключа Пользователь связывается с Оператором по телефону и сообщает ему следующие сведения:

- Свои идентификационные данные;
- Серийный номер сертификата ключа подписи, соответствующего скомпрометированному ключу;
- Секретное ключевое слово, полученное при регистрации.

Оператор производит аутентификацию Пользователя Удостоверяющего центра по секретному ключевому слову.

В случае успешной аутентификации Оператор приостанавливает действие сертификата на 30 (тридцати) календарных дней.

Если в течение срока приостановления действия сертификата ключа подписи Пользователь не направит в Удостоверяющий центр заявление на возобновление действия сертификата, то Удостоверяющий центр автоматически аннулирует (отзовет) данный сертификат.

Пользователь Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с пунктом 9.2.1 настоящего Регламента.

11.4. Конфиденциальность информации

11.4.1. Типы конфиденциальной информации

11.4.1.1.Закрытый ключ, соответствующий сертификату ключа подписи является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Оператор не осуществляет хранение закрытых ключей Пользователей Удостоверяющего центра.

11.4.1.2.Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре и содержащаяся в Реестре Удостоверяющего Центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа подписи, считается конфиденциальной.

11.4.2. Типы информации, не являющейся конфиденциальной

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

11.4.2.2.Открытая информация может публиковаться по решению Оператора и Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Оператором и Удостоверяющим центром.

11.4.2.3.Информация, включаемая в сертификаты ключей подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

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

11.4.3. Исключительные полномочия Оператора и Удостоверяющего центра

11.4.3.1.Оператор и Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях установленных законодательством Российской Федерации.

11.5. Форс-мажор

11.5.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

11.5.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

11.5.3. В случае возникновения форс-мажорных обстоятельств, срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

11.5.4. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

11.5.5. Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

11.5.6. В случае если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше 1 (одного) месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

12. Список приложений

12.1. Приложение №1. Заявление о присоединении к Регламенту предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».

12.2. Приложение №2. Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «КРИПТО-ПРО», определяющих отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение.

12.3. Приложение №3. Заявление на регистрацию Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО».

12.4. Приложение №4. Форма доверенности Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» на осуществление действий в рамках Регламента предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».

12.5. Приложение №5. Форма доверенности на осуществление регистрации Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО».

12.6. Приложение №6. Заявление на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.7. Приложение №7. Форма доверенности на получение ключей подписи и сертификата Пользователя в Удостоверяющем центре.

12.8. Приложение №8. Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.9. Приложение №9. Заявление на приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.10. Приложение №10. Заявление на возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.11. Приложение №11. Копия сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» (Пример).

Приложение №1 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

Заявление о присоединении к Регламенту предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО»

_____

(полное наименование организации, включая организационно-правовую форму)

зарегистрированное по адресу:

_____

(местонахождения, указанное в учредительных документах)

в лице

_____

(должность)

_____

(фамилия, имя, отчество)

действующего на основании

_____

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» (далее Регламент),
схема обслуживания:

_____

(централизованная или распределенная)

условия которого определены КИВИ Банк (АО) и опубликованы на сайте Оператора Удостоверяющего центра ООО «КРИПТО-ПРО». С настоящим Регламентом и приложениями к нему ознакомлен, обязуется соблюдать все положения указанного документа и является Стороной Регламента с момента подписания настоящего Заявления.

_____ _____ _____ «___»_____20__г.

(Должность) (ФИО) (Подпись) (Дата)

М.П.

Приложение №2 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО «КРИПТО-ПРО», определяющих отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение

	OID	Область применения
1.	1.2.643.2.2.34.5	Оператор Центра Регистрации – формирование электронной подписи электронных документов, определенных Регламентом для Оператора Удостоверяющего центра
2.	1.2.643.2.2.34.6	Пользователь Центра Регистрации – 1. Формирование электронной подписи электронных документов, определенных Регламентом для Пользователя Удостоверяющего центра 2. Формирование электронной подписи электронных документов, циркулирующих в *Информационной системе*

Приложение №3 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

Заявление на регистрацию Пользователя в Удостоверяющем центре ООО «КРИПТО-ПРО»

_____
(полное наименование организации, включая организационно-правовую форму)

в лице
_____
(должность)

_____
(фамилия, имя, отчество)
действующего на основании
_____

Просит зарегистрировать уполномоченного представителя

_____
(фамилия, имя, отчество)

в Реестре Удостоверяющего центра ООО «КРИПТО-ПРО» и наделить полномочиями Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», установленными Регламентом предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».

Настоящим
_____
(фамилия, имя, отчество)

соглашается с обработкой своих персональных данных Удостоверяющим центром ООО «КРИПТО-ПРО» и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Подпись уполномоченного представителя организации _____ /_____/
«____» _____ 20___
г.

_____ «___»_____20__г.
(Должность) (ФИО) (Подпись) (Дата)

м.п.

Приложение №4 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

(Форма доверенности Пользователя Удостоверяющего центра)

Доверенность

г. _____ «_____» _____20___ г.

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

выступать в роли Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» и осуществлять действия в рамках Регламента предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО», установленные для Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».
Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей Доверенностью.

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись уполномоченного представителя _____подтверждаю_____.
(Фамилия ИО) (подпись)

Руководитель организации

_____ «___»_____20__г.
(Должность) (ФИО) (Подпись) (Дата)

м.п.

Приложение №5 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

(Форма доверенности на осуществление регистрации Пользователя в Удостоверяющем центре)

Доверенность

г. _____ «_____» _____20___ г.

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

1. Предоставить Оператору Удостоверяющего центра ООО «КРИПТО-ПРО» необходимые документы, определенные Регламентом предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» для регистрации своего полномочного представителя - Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(фамилия, имя, отчество Пользователя УЦ)

2. Получить сертификат ключа подписи уполномоченного лица Удостоверяющего центра ООО «КРИПТО-ПРО» и иные документы, определенные Регламентом предоставления услуг Оператора Удостоверяющего центра ООО «КРИПТО-ПРО».

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.
Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись уполномоченного представителя _____подтверждаю_____.
(Фамилия ИО) (подпись)

Руководитель организации

_____ «___»_____20__г.
(Должность) (ФИО) (Подпись) (Дата)

м.п.

Приложение №6 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

Заявление на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(полное наименование организации, включая организационно-правовую форму)

в лице
_____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании
_____

Просит изготовить сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CommonName (CN)	Общее имя – Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Locality (L)	Город	
State (S)	Область	
Contry (C)	Страна	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6)

 Изготовить сертификат ключа подписи с генерацией ключей
 Изготовить сертификат ключа подписи в соответствии с предоставленным бланком запроса на сертификат ключа подписи*

Примечание:* - установить указатель в одно из указанных положений

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления

Печать организации

Бланк запроса на сертификат ключа подписи:
Наименование организации-Удостоверяющего Центра

Сведения о запросе на сертификат:
Этот запрос:
Кем выпущен:
User1
Версия: 1 (0x0)
Субьект запроса на сертификат: CN = User1
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-94
Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01
Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C 7DF9 F764 7822 99AA 3C3D 1E23 FE69 B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180 7CD3 ADD1 6D0E 00C9 9CA0 432F 595F 9CD3 12BE 69E6 A4D6 6133 227C DE1A 80F4 D0F1 8337 843E CAD1 561F 793B CB05 EEBB EBD4 C23F E5EA ECD9 E6B5 A9
Атрибуты запроса на сертификат X.509
1. Атрибут 1.3.6.1.4.1.311.13.2.3
Название: Версия ОС
Значение: 5.0.2195.2
2. Атрибут 1.3.6.1.4.1.311.2.1.14
Название: Расширения сертификатов
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 1.2.840.113549.1.9.15
Название: Возможности SMIME
Значение: [1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21
3. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Пользователь Центра Регистрации(1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2) Защищенная электронная почта(1.3.6.1.5.5.7.3.4)
3. Атрибут 1.3.6.1.4.1.311.13.2.2
Название: CSP заявки
Сведения о провайдере
Назначение ключа : ОБМЕН
Название провайдера : Crypto-Pro GOST R 34.10-94 Cryptographic Service Provider
Подпись провайдера : AA03 C083 A1B5 CCDC 20A0 F6A9 29D0 F124 8374 2251 6F71 C51A 52D5 469B 684B 7B7D 342F E0D8 8DDB 09EB B3BF 8DA6 3C98 AF07 327E 7EEB A121 A372 CA57 030A 87D2 AFA9 CDBB D3AA 7575 AA85 01B7 0AB3 79B5 98BA 8453 9B62 AA33 AA4C F07E 6043 64AB BCA5 0A4B EB59 A3D0 E55B D306 78A8 0B0B B05E 79F0 9001 E7B1 E133 B708 C11D 6AA1 4423 0000 0000 0000 0000
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-94
Параметры: 0500
Значение: BABC 1455 ADA3 DC7F 0EC9 3A1A 5020 C0DE F561 C757 2986 BB2E B180 A5B0 091A 7F0A 6FA1 1A6E EE48 A366 B904 7288 A311 D966 BB2F FC7C EB75 3F0A 49ED A651 3E10 258A

Подпись владельца запроса на сертификат: _____/_____

"___" _____ 20__ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Приложение №7 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

(Форма доверенности на получение ключей подписи и сертификата Пользователя в Удостоверяющем центре)

Доверенность

г. _____ «_____» _____20___ г.

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

1. Получить изготовленные на имя _____
(фамилия, имя, отчество)

ключи подписи и сертификат ключа подписи, а также сертификата ключа подписи уполномоченного лица Удостоверяющего центра ООО «КРИПТО-ПРО».

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись представителя _____подтверждаю_____.
(Фамилия ИО) (подпись)

Пользователь Удостоверяющего центра_____ /_____/
(Подпись) (Фамилия И.О. Пользователя)

Руководитель организации

_____ «___»_____20__г.
(Должность) (ФИО) (Подпись) (Дата)

м.п.

Приложение №8 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

в связи с _____
(причина отзыва сертификата*)

Просит аннулировать (отозвать) сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи	
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Locality (L)	Город	
State (S)	Область	
Contry (C)	Страна	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6)

Руководитель организации

_____ «___»_____20__г.
(Должность) (ФИО) (Подпись) (Дата)

м.п.

Приложение №9 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

Заявление на приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(полное наименование организации, включая организационно-правовую форму)

в лице
_____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании
_____

Просит приостановить действие сертификата ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи	
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Locality (L)	Город	
State (S)	Область	
Contry (C)	Страна	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6)

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

Руководитель организации

_____ «___»_____20__г.
(Должность) (ФИО) (Подпись) (Дата)

м.п.

Приложение №10 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

Заявление на возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО»

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие сертификата ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи	
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Locality (L)	Город	
State (S)	Область	
Contry (C)	Страна	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6)

Подпись владельца сертификата ключа подписи _____ /_____/«____» _____ 20____ г.

Руководитель организации

_____ «___»_____20__г.
(Должность) (ФИО) (Подпись) (Дата)

м.п.

Приложение №11 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»

Копия сертификата ключа подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» (Пример)

Сведения о сертификате:
Этот сертификат:
Подтверждает удаленному компьютеру идентификацию вашего компьютера
Защищает сообщения электронной почты
Пользователь Центра Регистрации
Кому выдан:
Фамилия Имя Отчество
Кем выдан:
CryptoPro CA
Действителен с 15 октября 2003 г. 12:03:00 UTC по 15 октября 2004 г. 12:12:00 UTC
Версия: 3 (0x2)
Серийный номер: 14F5 9CF2 0000 0000 003A
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Издатель сертификата: CN = CryptoPro CA, C = RU
Срок действия:
Действителен с: 15 октября 2003 г. 12:03:00 UTC
Действителен по: 15 октября 2004 г. 12:12:00 UTC
Владелец сертификата: CN = User1
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-94
Идентификатор: 1.2.643.2.2.20
Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01
Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C 7DF9 F764 7822 99AA 3C3D 1E23 FE69 B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180 7CD3 ADD1 6D0E 00C9 9CA0 432F 595F 9CD3 12BE 69E6 A4D6 6133 227C DE1A 80F4 D0F1 8337 843E CAD1 561F 793B CB05 EEBB EBD4 C23F E5EA ECD9 E6B5 A9
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Защищенная электронная почта(1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации(1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 56BD CA83 3029 0673 CA83 3381 16D4 AF10 C3D6 9A75
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=50AA 3E1E 4186 F8DC 3585 6E11 2C11 D9E3 0A91 7AD7 Поставщик сертификата: Адрес каталога: CN=CryptoPro CA C=RU Серийный номер сертификата=29D1 B0C8 C311 ACAE 48DB AAB1 3687 CEFC
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Значение: 826C DDFB 331C 58C5 FD3D 9233 4A1D 2D7A B973 387C 8E8A DD3D 6FCE 0573 508A 3DC4 B29F 5961 FB6C D1EB 1B40 37C7 8473 5B0F FECA 5E38 EA0C 3890 C77A C97E BD18 873A

Ответственный сотрудник Оператора Удостоверяющего центра _____/_____«____» _____ 20__ г.

Печать Оператора УЦ

Подпись владельца сертификата ключа подписи: _____/_____«____» _____ 20__ г.