УТВЕРЖДЕН
Приказом
Генерального директора
ООО «Системы распределенного реестра»
от «25» июля 2023 г. № 230725-Пр-1

РЕГЛАМЕНТ
Оператора Удостоверяющего центра
ООО «КРИПТО-ПРО»
(в новой редакции)

г. Москва, 2023

Термины и определения

В настоящем Регламенте используются термины и определения, установленные Федеральным законом от 06.04.2011 № 63- ФЗ «Об электронной подписи», а также термины и определения их дополняющие и конкретизирующие, а именно:

Владелец сертификата ключа проверки электронной подписи – лицо, которому в соответствии с законодательством Российской Федерации и настоящим Регламентом выдан сертификат ключа проверки электронной подписи.

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

Ключ электронной подписи действует на определенный момент времени (действующий ключ электронной подписи) если:

- наступил момент времени начала действия ключа электронной подписи;
- срок действия ключа электронной подписи не истек;
- сертификат ключа проверки электронной подписи, соответствующий данному ключу электронной подписи, действует на указанный момент времени.

Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, заверенный собственноручной подписью ответственного лица Оператора Удостоверяющего центра и заверенный печатью Оператора Удостоверяющего центра. Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи. Структура копии сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

Оператор Удостоверяющего центра (Оператор УЦ, Оператор) – ООО «Системы распределенного реестра» (далее - Общество), наделенное Удостоверяющим центром полномочиями по обеспечению создания ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, управлению (выдача, аннулирование, прекращение, приостановление и возобновление действия) сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра и уполномоченная Удостоверяющим центром заверять копии сертификатов ключей проверки электронной подписи на бумажном носителе, выданных Оператором предоставления услуг Удостоверяющего центра.

Пользователь Удостоверяющего центра (Пользователь УЦ) – физическое лицо, являющееся владельцем ключа проверки электронной подписи, либо физическое лицо, действующее от имени юридического лица, являющегося владельцем ключа проверки электронной подписи, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием этого юридического лица.

Рабочий день Оператора Удостоверяющего центра (далее – рабочий день) – промежуток времени с 10:00 по 18:00 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

Сертификат ключа проверки электронной подписи – электронный документ, выданный Оператором Удостоверяющего центра или доверенным лицом Оператора

Удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи действует на определенный момент времени (действующий сертификат) если:

- наступил момент времени начала действия сертификата ключа проверки электронной подписи;
- срок действия сертификата ключа проверки электронной подписи не истек;
- сертификат ключа проверки электронной подписи не аннулирован, не прекратил действие и действие его не приостановлено.

Служба актуальных статусов сертификатов – сервис Удостоверяющего центра (построенный на базе протокола OCSP), с использованием которого подписываются электронной подписью и предоставляются Пользователям УЦ электронные ответы, содержащие информацию о статусе сертификатов ключей проверки электронной подписи, выданных Удостоверяющим центром.

Служба штампов времени – сервис Удостоверяющего центра (построенный на базе протокола TSP), с использованием которого подписываются электронной подписью и предоставляются Пользователям УЦ штампы времени.

Список отозванных сертификатов (СОС) – электронный документ с электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на этот определенный момент времени аннулированы, действие которых прекращено и действие которых приостановлено.

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

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

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 электронной подписи.

Псевдоним владельца сертификата ключа проверки электронной подписи – вымышленное имя физического лица, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре.

Удостоверяющий центр – ООО «КРИПТО-ПРО», осуществляющее выполнение целевых функций удостоверяющего центра по изготовлению и управлению неквалифицированными сертификатами ключей проверки электронной подписи в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи» в целях обеспечения применения участниками Информационной системы неквалифицированной усиленной электронной подписи.

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

- реестр заявлений на регистрацию пользователей в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление сертификата ключа проверки электронной подписи;
- реестр заявлений на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи;
- реестр заявлений на приостановление/возобновление действия сертификата ключа проверки электронной подписи;
- реестр заявлений на подтверждение подлинности электронной подписи электронного документа;
- реестр заявлений на подтверждение электронной подписи Уполномоченного лица Удостоверяющего центра в изданных сертификатах;
- реестр сертификатов ключей проверки электронной 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 электронной подписи и списков отозванных сертификатов.

Информационная система - корпоративная информационная система, устроителем которой является организатор системы, в которой используются закрытые ключи и сертификаты открытых ключей проверки электронной подписи, и предоставляющая определенные услуги участникам этой системы.

Cryptographic Message Syntax (CMS) – стандарт, определяющий формат и синтаксис криптографических сообщений.

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

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

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий Центр осуществляет свою работу в соответствии со следующим стандартом PKCS - PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа.

1. Сведения об Операторе Удостоверяющего центра

ООО «Системы распределенного реестра», именуемое в дальнейшем «Оператор Удостоверяющего центра» («Оператор»), зарегистрировано на территории Российской Федерации. Лист записи Единого государственного реестра юридических лиц о внесении записи о создании юридического лица 04 мая 2021 за государственным регистрационным номером 1217700216360.
Оператор в качестве профессионального участника рынка услуг по созданию и выдаче сертификатов ключей проверки электронных подписей осуществляет свою деятельность на территории Российской Федерации на основании следующей лицензии:
Лицензия ФСБ России 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).
Сведения об указанной лицензии содержатся в Реестре лицензий на деятельность, связанную с шифровальными (криптографическими) средствами, ведение которого осуществляется ФСБ России, доступном в сети Интернет по адресу http://clsz.fsb.ru/clsz/license.htm

Реквизиты Оператора:
Полное наименование: Общество с ограниченной ответственностью «Системы распределенного реестра»
Юридический адрес: 121099, г. Москва, вн. тер. г. муниципальный округ Арбат, ул. Композиторская, д. 17, эт./пом. 7/I, ком. 11-17
Фактический адрес: 121099, г. Москва, вн. тер. г. муниципальный округ Арбат, ул. Композиторская, д. 17, эт./пом. 7/I, ком. 11-17
Адрес для корреспонденции: 121099, г. Москва, вн. тер. г. муниципальный округ Арбат, ул. Композиторская, д. 17, эт./пом. 7/I, ком. 11-17
Банковские реквизиты (наименование банка, БИК, р/с, к/с):

- Филиал «ЦЕНТРАЛЬНЫЙ» Банка ВТБ (ПАО) г. Москва
- БИК 044525411
- Р/с 40702810037000002721
- К/с 30101810145250000411

ИНН/КПП: 9704063885 / 770401001
ОГРН: 1217700216360
ОКВЭД: 62.01
ОКПО: 60003364

Контактные телефоны, факс, адрес электронной почты:

- тел./факс: +7 (495) 120-75-42;
- e-mail: ca@masterchain.ru

1. Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью «КРИПТО-ПРО», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва. Свидетельство о регистрации № 001.602.749, выдано 16.11.1999г. Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003г., Свидетельство о внесении записи в ЕГРЮЛ в связи с государственной

регистрацией изменений, вносимых в учредительные документы юридического лица за государственным регистрационным номером 2037719011031 от 12.03.2003г.

Удостоверяющий центр в качестве профессионального участника рынка услуг по изготовлению и выдаче сертификатов открытых ключей осуществляет свою деятельность на территории Российской Федерации на основании следующей лицензии:

Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России рег. № 12936 Н от 11 июня 2013 г. 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).

Контактные телефоны, адрес электронной почты:

- тел.: +7 (495) 995-48-20.
- e-mail: cpca@cryptopro.ru; cpca20@cryptopro.ru

2. Присоединение к Регламенту

2.1. Настоящий Регламент со всеми приложениями к нему является договором присоединения в соответствии со ст. 428 Гражданского кодекса РФ.

2.2. Присоединение к настоящему Регламенту осуществляется путем подачи Заявителем заявки на регистрацию в Удостоверяющем центре в порядке, определенном разделом 9 настоящего Регламента. С момента подачи заявки Заявитель считается присоединившимся к Регламенту и становится стороной Регламента – Пользователем Удостоверяющего центра.

2.3. Факт присоединения Заявителя к Регламенту является полным принятием им условий настоящего Регламента и всех его положений в редакции, действующей на момент подачи заявки на регистрацию в Удостоверяющем центре. Сторона, присоединившаяся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

3. Общие положения

3.1. Статус Регламента

3.1.1. Регламент Оператора Удостоверяющего центра ООО «КРИПТО-ПРО» по созданию и управлению сертификатами ключей проверки электронной подписи (распределенная схема обслуживания), именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

3.1.2. Сторонами Регламента (далее Стороны) являются ООО «Системы распределенного реестра», выступающая Оператором Удостоверяющего центра, и Сторона, присоединившаяся к Регламенту.

3.1.3. Настоящий Регламент распространяется в форме электронного документа по адресу: https://dltru.org/ca/reglament_ca.pdf

3.2. Применение Регламента

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

3.2.2. 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.

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

3.3. Изменение (дополнение) Регламента

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

3.3.2. Уведомление о внесении изменений в Регламент осуществляется Оператором путем обязательного размещения указанных изменений на сайте Оператора.

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

3.3.4. 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) направить заявление на расторжение отношений в форме электронного письма на адрес Оператора Удостоверяющего центра.

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

4. Основания осуществления деятельности Удостоверяющего центра

4.1. Удостоверяющий центр осуществляет свою деятельность в соответствии с лицензией ФСБ России на право осуществления технического обслуживания шифровальных (криптографических) средств, распространения шифровальных (криптографических) средств, оказания услуг в области шифрования информации и аккредитацией Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. С копиями указанных документов Сторона, присоединившаяся к Регламенту, может ознакомиться по следующему адресу в сети Интернет - http://www.cryptopro.ru/about/licenses.

5. Права и обязанности Сторон

5.1. Оператор обязан:

5.1.1. Установить личность заявителя - физического лица, обратившегося к нему за получением сертификата ключа проверки электронной подписи, получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением сертификата ключа проверки электронной подписи.

5.1.2. Предоставить Удостоверяющему центру информацию для регистрации пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.3. По запросу предоставить Пользователю Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме.

5.1.4. Использовать сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

5.1.5. Принимать меры по защите передаваемых данных Пользователя Удостоверяющему центру и ключа электронной подписи от несанкционированного доступа.

5.1.6. Организовать свою работу по московскому времени.

5.1.7. Оператор обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

5.1.8. Обеспечить уникальность идентификационных данных Пользователей Удостоверяющего центра, заносимых в сертификаты ключей проверки электронной подписи.

5.2. Сторона, присоединившаяся к Регламенту, обязана:

5.2.1. Известить Удостоверяющий центр об изменениях в наименовании Организации, основного государственного регистрационного номера, идентификационного номера налогоплательщика и т.д..

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

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

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

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

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

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

5.2.2.6. Немедленно обратиться к Оператору с заявлением на приостановление действия сертификата ключа проверки электронной подписи в случае потери, раскрытия, искажения личного закрытого ключа электронной подписи, а также в

случае если Пользователю Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами.

5.2.2.7. Оповестить Оператора в случае, если подано заявление об аннулировании сертификата электронной подписи.

5.2.2.8. Самостоятельно ознакомиться с Регламентом https://dltru.org/ca/reglament_ca.pdf.

5.3. Оператор имеет право:

5.3.1. Отказать в регистрации Пользователя Удостоверяющего центра уполномоченному представителю Стороны, в случае ненадлежащего оформления заявления на изготовление сертификата ключа проверки электронной подписи и/или необходимых документов.

5.3.2. Отказать в приостановлении /возобновлении действия или аннулировании/прекращении действия (отзыве) подачи заявки на аннулирование сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи.

5.3.3. Отказать в прекращении действия (отзыве) сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа электронной подписи, соответствующего этому сертификату ключа проверки электронной подписи.

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

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

5.3.6. Запрашивать у Заявителей документы для подтверждения сведений, представленных ими при обращении в Удостоверяющий центр.

5.3.7. Запросить у Заявителя дополнительные, подтверждающие достоверность представленных им сведений, документы.

5.3.8. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Пользователя УЦ с обязательным уведомлением, когда Пользователь УЦ действует от имени юридического лица, владельца сертификата ключа проверки электронной подписи, действие которого приостановлено, в случае нарушения таким Пользователем УЦ требований правил Автоматизированных систем (АС), в которых Оператор выполняет функции администратора (согласно перечню АС, указанному в Приложении № 10).

5.3.9. Отказать в изготовлении сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если использованное Пользователем Удостоверяющего центра для формирования запроса на сертификат ключа проверки электронной подписи средство криптографической защиты информации не поддерживает формат запроса, установленный Удостоверяющим центром.

5.3.10. Отказать в изготовлении сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если использованное Пользователем Удостоверяющего центра для формирования запроса на сертификат ключа проверки электронной подписи средство криптографической защиты информации не поддерживает формат запроса, установленный Удостоверяющим центром.

5.3.11. Вносить изменения в Регламент в одностороннем порядке.

6. Вознаграждение Оператора Удостоверяющего центра. Сроки и порядок расчетов.

6.1. Вознаграждение Оператора за изготовление одного сертификата ключа проверки электронной подписи (клиентский сертификат ключа проверки электронной подписи, структура которого определена пунктом 11.2 настоящего Регламента) составляет 1 500 (одна тысяча пятьсот) рублей 00 копеек, без учёта НДС. НДС рассчитывается в соответствии со ставкой, установленной законодательством Российской Федерации.

6.2. Вознаграждение Оператора за изготовление одного сертификата ключа проверки электронной подписи (серверный сертификат ключа проверки электронной подписи, структура которого определена пунктом 11.2 настоящего Регламента) составляет 14 500 (четырнадцать тысяч пятьсот) рублей 00 копеек, без учёта НДС. НДС рассчитывается в соответствии со ставкой, установленной законодательством Российской Федерации.

6.3. За изготовление сертификатов ключей проверки электронной подписи, вызванных внеплановой сменой ключей Пользователей УЦ, связанной с компрометацией ключей Уполномоченного лица Удостоверяющего центра (пункт 12.2 настоящего Регламента), плата не взимается.

7. Ответственность сторон

7.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

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

7.3. 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 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 города Москвы.
Сторона, получившая от другой Стороны претензию, обязана в течение 20 (Двадцати) рабочих дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

9. Порядок предоставления и пользования услугами Удостоверяющего центра

9.1. Регистрация Пользователей Оператором УЦ

9.1.1. Регистрация пользователя и изготовление первого сертификата ключа проверки электронной подписи в распределенном режиме:

Регистрация Пользователя Удостоверяющего центра осуществляется на основании заявки на регистрацию в Удостоверяющем центре, содержащей регистрационные данные Заявителя, включая информацию, подлежащую внесению в сертификат. Заявка подается Заявителем в форме электронного документа через личный кабинет Пользователя в информационной системе Удостоверяющего центра.

После принятия положительного решения о регистрации и прохождении идентификации сотрудник Оператора осуществляет регистрацию пользователя УЦ и направляет временный пароль для создания запроса на сертификат и/или регистрирует пользователя, предоставляет пользователю сертификат ключа проверки электронной подписи.

Пользователь производит установку и настройку своего рабочего места и с помощью автоматизированного рабочего места (АРМ) Пользователя Удостоверяющего центра формирует и может самостоятельно направить запрос на регистрацию в электронной форме в Удостоверяющий центр.

Регистрация Пользователя должны быть осуществлены не позднее 3-х 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 генерирует пару ключей, формирует и направляет запрос на изготовление сертификата ключа проверки электронной подписи в электронной форме в Удостоверяющий центр.

Сотрудник Оператора производит сравнение идентификационной информации, указанной в заявлении пользователя с информацией, содержащейся в запросе на регистрацию, поданном в электронной форме. В случае идентичности указанной идентификационной информации пользователь регистрируется Оператором в Удостоверяющем центре. В случае идентичности идентификационной информации ответственное лицо издает сертификат открытого ключа пользователя и направляет в электронном или печатном виде сведения о сертификате открытого ключа. Экземпляр визируется ответственным сотрудником Оператора Удостоверяющего центра в случае если это электронный документ. В случае, если бумажная версия, то печатается в 2х экземплярах, визируются ответственным сотрудником Оператора Удостоверяющего центра, заверяются печатью Оператора Удостоверяющего центра и посредством почтовой или курьерской связи предоставляются пользователю Удостоверяющего центра.

Изготовление сертификата ключа проверки электронной подписи должно быть осуществлено не позднее 3-х рабочих дней, следующих за рабочим днем, в течение которого был подан запрос на изготовление сертификата ключа проверки электронной подписи в электронном виде.

После получения уведомления об изготовлении сертификата ключа проверки электронной подписи пользователь с помощью АРМ пользователя Удостоверяющего центра вводит секретную ключевую фразу, производит установку сертификата ключа проверки электронной подписи на своем рабочем месте и подтверждает ее.

До истечения 30-ти календарных дней с момента получения уведомления об изготовлении сертификата ключа проверки электронной подписи пользователь должен подписать и соответствующим образом заверить электронную версию

(бумажную в двух экземплярах) сертификата открытого ключа и предоставить Оператору один экземпляр.

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

9.2.1. Изготовление и получение сертификата ключа проверки электронной подписи по заявлению, поданному в бумажной форме:
Форма заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи приведена в Приложении № 3 к настоящему Регламенту.
В том случае, если Пользователь УЦ не может прибыть лично в офис Оператора, должна быть осуществлена идентификация Пользователя иными способами.
Оператор УЦ при личном посещении выполняет процедуру идентификации Пользователя УЦ путем установления личности по паспорту.
После положительной идентификации Пользователя УЦ или доверенного лица сотрудник Оператора принимает документы и осуществляет их рассмотрение.
Заявление на изготовление ключей подписи и сертификата открытого ключа рассматривается Оператором 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 Оператора Удостоверяющего центра.
При принятии положительного решения сотрудник Оператора Удостоверяющего центра изготавливает ключи подписи и сертификат ключа проверки электронной подписи на предоставляемый Пользователем УЦ или его представителем ключевой носитель.

9.2.2. Изготовление и получение сертификата ключа проверки электронной подписи по заявлению, поданному в электронной форме:
Подача Пользователем УЦ заявления на изготовление сертификата ключа проверки электронной подписи в электронной форме осуществляется с использованием программного обеспечения, предоставляемого Удостоверяющим центром.
Заявление на изготовление сертификата ключа проверки электронной подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на сертификат ключа проверки электронной подписи в формате PKCS#10, а электронная подпись осуществляется на действующем закрытом ключе Пользователя УЦ.
Значения полей Subject, Key Usage, Extended Key Usage, содержащиеся в запросе на сертификат должны быть идентичны значениям этих полей в сертификате ключа проверки электронной подписи, соответствующего закрытому ключу Пользователя

УЦ, которым сформирована электронная подпись на заявлении на изготовление сертификата ключа проверки электронной подписи Пользователя УЦ.
После регистрации отправленного заявления в Удостоверяющем центре сотрудник Оператора 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 проверки электронной подписи автора настоящего заявления.
В случае отрицательного результата проведенных проверок, а также иных случаях, установленных настоящим Регламентом, сотрудник Оператора УЦ отклоняет заявление на изготовление сертификата ключа проверки электронной подписи.
Срок рассмотрения заявления на изготовление сертификата ключа проверки электронной подписи составляет один рабочий день с момента регистрации заявления на изготовление сертификата ключа проверки электронной подписи в УЦ. В случае отказа в изготовлении сертификата ключа проверки электронной подписи сотрудник Оператора УЦ официально уведомляет Пользователя УЦ об этом в срок, установленный для рассмотрения заявления.
При принятии положительного решения сотрудник Оператора УЦ принимает заявление на изготовление сертификата ключа проверки электронной подписи и осуществляет изготовление сертификата ключа проверки электронной подписи.
Срок изготовления сертификата ключа проверки электронной подписи составляет 3 (Три) рабочих дня с момента регистрации заявления на сертификат ключа проверки электронной подписи в Удостоверяющем центре. После изготовления сертификата ключа проверки электронной подписи Удостоверяющий центр официально уведомляет по электронной почте Пользователя УЦ об этом, после чего Пользователь УЦ устанавливает сертификат ключа проверки электронной подписи на своем рабочем месте с использованием предоставленного Удостоверяющим центром программного обеспечения.
Дополнительно Оператор УЦ формирует и направляет Пользователю УЦ два экземпляра копии сертификата ключа проверки электронной подписи, подписанные Оператором УЦ и заверенные печатью Оператора УЦ.
До истечения 30-ти календарных дней с момента официального уведомления пользователя об изготовлении сертификата ключа проверки электронной подписи Пользователь УЦ должен подписать два экземпляра копии сертификата ключа проверки электронной подписи и предоставить Оператору УЦ один экземпляр.

9.3. Аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи Пользователя УЦ:
Для осуществления аннулирования/прекращения действия (отзыва) сертификата ключа проверки электронной подписи Пользователь УЦ подает заявление на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи Оператору УЦ.
Заявление на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи может подаваться в бумажной форме (при личном прибытии Пользователя УЦ в офис Оператора, 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/прекращение действия (отзыв) сертификата ключа проверки электронной подписи по заявлению, поданному в бумажной форме:
Форма заявления на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи приведена в Приложении № 4 к настоящему Регламенту.
Заявление на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи заверяется собственноручной подписью владельца

сертификата ключа проверки электронной подписи (Пользователя УЦ) и подается в офис Оператора предоставления услуг Удостоверяющего центра.
Подача заявления и его рассмотрение осуществляется только в течение рабочего дня Оператора УЦ.
Обработка заявления на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи и официальное уведомление Пользователя УЦ об аннулировании/прекращение действия (отзыве) сертификата ключа проверки электронной подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление Оператору УЦ.
Официальным уведомлением о факте аннулирования/прекращения действия (отзыва) сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения об отозванном сертификате. Временем аннулирования/прекращения действия (отзыва) сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения об отозванном сертификате, указанное в поле thisUpdate изданного списка отозванных сертификатов.
Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа проверки электронной подписи в поле CRL Distribution Point.

9.3.2. Аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи по заявлению, поданному в электронной форме:
Подача Пользователем УЦ заявления на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи в электронной форме осуществляется с использованием программного обеспечения, предоставляемого Удостоверяющим центром.
Заявление на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи Пользователя УЦ в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на отзыв сертификата ключа проверки электронной подписи, а электронная подпись осуществляется на действующем закрытом ключе Пользователя УЦ.
Запрос на отзыв сертификата ключа проверки электронной подписи представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер отзываемого сертификата ключа проверки электронной 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 проверки электронной подписи.

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

В случае отрицательного результата проведенных проверок, а также иных случаях, установленных настоящим Регламентом, Оператор УЦ отклоняет заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи.
Срок рассмотрения заявления на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи составляет один рабочий день с момента регистрации заявления в Удостоверяющем центре. В случае отказа в аннулировании/прекращении действия (отзыве) сертификата ключа проверки электронной подписи Оператор УЦ официально уведомляет Пользователя УЦ об этом в срок, установленный для рассмотрения заявления.
При принятии положительного решения Оператор УЦ отзывает сертификат ключа проверки электронной подписи.
Обработка заявления на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи и официальное уведомление Пользователя УЦ об аннулировании/прекращении действия (отзыве) сертификата ключа проверки электронной 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/прекращения действия (отзыва) сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения об отозванном сертификате. Временем аннулирования/прекращения действия (отзыва) сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения об 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 проверки электронной подписи Пользователя Удостоверяющего центра:
Для осуществления приостановления действия сертификата ключа проверки электронной подписи Пользователь УЦ подает заявление на приостановление действия сертификата ключа проверки электронной подписи.
Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется Оператором УЦ на основании заявления, поступающего в устной, бумажной или электронной форме.
Заявитель должен сообщить ответственному сотруднику Оператора УЦ следующую информацию:

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

Заявление на приостановление действия сертификата ключа проверки электронной подписи 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 УЦ по форме, определенной Приложением № 5.
Заявление в бумажной форме содержит следующую информацию:

- идентификационные данные владельца сертификата ключа проверки электронной подписи;

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

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

Заявление на приостановление действия сертификата ключа проверки электронной 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 на действующем закрытом ключе 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 проверки электронной подписи.

Заявление на приостановление действия сертификата ключа проверки электронной подписи в электронном виде формируется и подается в Удостоверяющий центр с использованием программного обеспечения, предоставляемого Удостоверяющим центром.

После регистрации отправленного заявления в Удостоверяющем центре Оператор УЦ проверяет корректность электронной подписи заявления и устанавливает его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа проверки электронной подписи (сертификата ключа проверки электронной подписи, действие которого требуется приостановить), серийный номер которого указан в запросе на приостановление действия сертификата ключа проверки электронной 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 проверки электронной 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 проверки электронной подписи является опубликование списка отозванных

сертификатов, содержащего сведения о сертификате, действие которого было приостановлено. Временем приостановления действия сертификата ключа проверки электронной 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 проверки электронной подписи Пользователя УЦ Оператору УЦ не поступает заявление от Пользователя УЦ о возобновлении действия сертификата ключа проверки электронной подписи, сертификат отзывается Удостоверяющим центром.

9.5. Возобновление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра:
Для осуществления возобновления действия сертификата ключа проверки электронной подписи Пользователь УЦ подает заявление на возобновление действия сертификата.
Возобновление действия сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется Оператором УЦ на основании заявления на возобновление действия сертификата ключа проверки электронной подписи, поступающего в бумажной или электронной форме.
Заявление в бумажной форме подается в офис Оператора УЦ по форме, определенной Приложением № 6.
Заявление в бумажной форме содержит следующую информацию:

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

Заявление на возобновление действия сертификата ключа проверки электронной подписи в бумажной форме заверяется собственноручной подписью владельца сертификата (Пользователя УЦ) и подается в офис Оператора УЦ (при личном прибытии заявителя, либо посредством почтовой или курьерской связи).
Заявление на возобновление действия сертификата ключа проверки электронной 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 на действующем закрытом ключе Пользователя УЦ.
Запрос на возобновление действия сертификата представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер сертификата ключа проверки электронной подписи, действие которого требуется возобновить;
- ReasonCode – «-1» - возобновление действия;
- SomeComment - текстовое значение комментария владельца сертификата ключа проверки электронной 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 Оператор УЦ проверяет корректность электронной подписи на заявлении и устанавливает его автора, затем устанавливает – является ли автор заявления владельцем сертификата ключа проверки электронной подписи (сертификата ключа проверки электронной подписи, действие которого требуется возобновить), серийный номер которого указан

в запросе на возобновление действия сертификата ключа проверки электронной 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 проверки электронной подписи является опубликование списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено. Временем возобновления действия сертификата ключа проверки электронной 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 проверки электронной 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 УЦ.
Подтверждение подлинности ЭП 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 проверки электронной 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 будет считаться равнозначной собственноручной подписи при выполнении следующих условий:

- сертификат ключа проверки электронной 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 на сертификате ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, верна;
- электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа проверки электронной 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 УЦ.
Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Оператора УЦ. При проведении указанных работ Оператор УЦ (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 УЦ.
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 использованных методов;
- обоснование результатов проверки;
- данные, представленные комиссии для проведения проверки;

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручной подписью каждого члена комиссии.

9.7. Подтверждение подлинности ЭП Уполномоченного лица Удостоверяющего центра в изданных сертификатах ключа проверки электронной подписи:
Для подтверждения подлинности ЭП Уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи Пользователь УЦ подает заявление на подтверждение подлинности ЭП Уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи Оператору УЦ.
Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные субъекта, в сертификате ключа проверки электронной подписи которого необходимо подтвердить ЭП уполномоченного лица Удостоверяющего центра;
- серийный номер сертификата ключа проверки электронной 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 проверки электронной подписи является сменный магнитный носитель, содержащий файл сертификата ключа проверки электронной 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 УЦ.
На основании полученного заявления Оператор УЦ установленным порядком обращается в Удостоверяющий центр, который осуществляет подтверждение

подлинности ЭП Уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи.
Результатом проведения работ по подтверждению подлинности ЭП Уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной 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 использованных 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 УЦ может быть осуществлена уполномоченным представителем Пользователя Удостоверяющего центра, действующим на основании доверенности на осуществление регистрации в Удостоверяющем центре.

9.8.2. Период времени действия закрытого ключа электронной подписи, соответствующего выданному сертификату ключа проверки электронной 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 проверки электронной подписи и сроки действия ключевых документов

10.1. Структура сертификата ключа проверки электронной 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 34.11/34.10-2012
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 UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
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 34.10-2012)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
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 проверки электронной 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 34.11/34.10-2012
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 UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
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 34.11/34.10-2012
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; электронная 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 проверки электронной 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 UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 10.3.1.1. Серийный номер сертификата (CertificateSerialNumber) 10.3.1.2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 10.3.1.3. 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 34.11/34.10-2012
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
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. Сроки действия ключевых документов

10.4.1. Срок действия закрытого ключа электронной подписи 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 электронной подписи Уполномоченного лица Удостоверяющего центра исчисляется с даты и времени генерации закрытого ключа Уполномоченного лица Удостоверяющего центра.
Срок действия сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

10.4.2. Срок действия закрытого ключа электронной подписи Пользователя Удостоверяющего центра составляет 1 (один) год.
Начало периода действия закрытого ключа электронной подписи Пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.
Срок действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной 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 электронной подписи Уполномоченного лица Удостоверяющего центра

Плановая смена ключей электронной подписи (закрытого и соответствующего ему открытого ключа) Уполномоченного лица Удостоверяющего центра выполняется в период действия закрытого ключа электронной подписи 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 проверки электронной подписи Уполномоченного лица Удостоверяющего центра

Старый закрытый ключ электронной подписи 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 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 Period сертификата ключа проверки электронной 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 электронной подписи Уполномоченного лица Удостоверяющего центра

В случае компрометации закрытого ключа электронной подписи 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 ключа проверки электронной подписи 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 центра.

Все действовавшие на момент компрометации закрытого ключа электронной подписи Уполномоченного лица Удостоверяющего центра сертификаты ключей проверки электронной подписи, 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 электронной подписи.

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

- Свои идентификационные данные;
- Серийный номер сертификата ключа проверки электронной 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 календарных дней.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи Пользователь не направит в Удостоверяющий центр заявление на возобновление действия сертификата, то Удостоверяющий центр автоматически прекратит действие (отзовет) данного сертификата.

11.4. Конфиденциальность информации

11.4.1. Типы конфиденциальной информации.

11.4.1.1. Закрытый ключ, соответствующий сертификату ключа проверки электронной 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 проверки электронной 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. Персональные данные, включаемые в сертификаты ключей подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

11.4.2.5. 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 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. 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.

12.2. Приложение №2. Форма доверенности Пользователя Удостоверяющего центра.

12.3. Приложение №3. Форма Заявления на изготовление неквалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.4. Приложение №4. Форма Заявления на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.5. Приложение №5. Форма Заявления на приостановление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.6. Приложение №6. Форма Заявления на возобновление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

12.7. Приложение №7. Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО»

12.8. Приложение №8. Форма заявления на проверку подлинности электронной подписи в электронном документе.

12.9. Приложение №9. Копия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (Пример).

12.10. Приложение №10. Перечень автоматизированных систем, в отношении которых ООО «Системы распределенного реестра» выполняет функции администратора автоматизированной системы.

Приложение №1 к Регламенту
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.	1.2.643.6.57.1.1.1.1	[TLS Server] Узел Мастерчейн
2.	1.2.643.6.57.1.1.1.2	[TLS Client] Узел Мастерчейн
3.	1.2.643.6.57.1.1.1.3	[TLS Server] API узла Мастерчейн
4.	1.2.643.6.57.1.2.1.1	[TLS Server] API СПКС
5.	1.2.643.6.57.1.2.1.2	[TLS Client] API СПКС
6.	1.2.643.6.57.1.3.1.3	[TLS Client] АРМ Администратора Мастерчейн
7.	1.2.643.6.57.1.4.1.1	[TLS Server] API Системы мониторинга
8.	1.2.643.6.57.1.4.1.2	[TLS Client] API Системы мониторинга
9.	1.2.643.6.57.1.4.1.3	[TLS Client] АРМ Системы мониторинга
10.	1.2.643.6.57.1.5.1.1	[TLS Server] API ИС
11.	1.2.643.6.57.1.5.1.2	[TLS Client] API ИС
12.	1.2.643.6.57.1.5.1.3	[TLS Client] АРМ ИС
13.	1.2.643.6.57.1.3.2.1	[Sign] Админ сети
14.	1.2.643.6.57.1.3.2.2	[Sign] Админ Whitelist
15.	1.2.643.6.57.1.4.2.1	[Sign] АРМ Мониторинга Мастерчейн
16.	1.2.643.6.57.1.4.2.2	[Sign] АРМ Мониторинга Мастерчейн Участник
17.	1.2.643.6.57.1.5.2.1	[Sign] АРМ ИС Админ
18.	1.2.643.6.57.1.5.2.2	[Sign] АРМ ИС робот
19.	1.2.643.6.57.1.5.2.3	[Sign] АРМ ИС Админ Банка
20.	1.2.643.6.57.1.5.2.4	[Sign] АРМ ИС Менеджер Банка
21.	1.2.643.6.57.1.2.2.1	[Sign] CMS Storage
22.	1.2.643.6.57.1.1.3.1	[Block Sign] Узел Мастерчейн
23.	1.2.643.6.57.1.2.4.1	[Encrypt Payload] CMS Storage Transport Key
24.	1.2.643.6.57.1.2.4.2	[Encrypt Payload] CMS IS Transport Key
25.	1.2.643.6.57.1.2.4.3	[Encrypt Payload] CMS IS User Transport Key
26.	1.2.643.6.57.1.2.1.1.1	[TLS Server] Узел Мастерчейн (ДДС 2.0)
27.	1.2.643.6.57.1.2.1.1.2	[TLS Client] Узел Мастерчейн (ДДС 2.0)
28.	1.2.643.6.57.1.2.1.1.3	[TLS Server] API узла Мастерчейн (ДДС 2.0)
29.	1.2.643.6.57.1.2.5.1.1	[TLS Server] API ИС (ДДС 2.0)
30.	1.2.643.6.57.1.2.5.1.2	[TLS Client] API ИС (ДДС 2.0)

31.	1.2.643.6.57.1.2.5.1.3	[TLS Client] АРМ ИС (ДДС 2.0)
32.	1.2.643.6.57.1.2.2.1.1	[TLS Server] API СПКС (ДДС 2.0)
33.	1.2.643.6.57.1.2.2.1.2	[TLS Client] API СПКС (ДДС 2.0)
34.	1.2.643.6.57.1.2.5.2.2	[Sign] АРМ ИС Робот (ДДС 2.0)
35.	1.2.643.6.57.1.2.5.2.3	[Sign] АРМ ИС Админ Банка (ДДС 2.0)
36.	1.2.643.6.57.1.2.5.2.4	[Sign] АРМ ИС Менеджер Банка (ДДС 2.0)
37.	1.2.643.6.57.1.2.2.2.1	[Sign] CMS Storage (ДДС 2.0)
38.	1.2.643.6.57.1.2.2.4.1	[Encrypt Payload] CMS IS (ДДС 2.0)
39.	1.2.643.6.57.1.2.2.4.2	[Encrypt Payload] CMS IS API Transport Key (ДДС 2.0)
40.	1.2.643.6.57.1.2.2.4.3	[Encrypt Payload] CMS IS User Transport Key (ДДС 2.0)
41.	1.2.643.6.57.1.2.1.3.1	[Block Sign] Узел Мастерчейн (ДДС 2.0)

Приложение №2 к Регламенту 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 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 Фамилия И.О. _____
подтверждаю.

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

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

Заявление на изготовление неквалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО».

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____
(Устава / Доверенности от _____ № ____)

Просит изготовить сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CommonName (CN)	Общее имя	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Locality (L)	Город	
State (S)	Область	
Contry (C)	RU	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4)
( )	[TLS Server] Узел Мастерчейн	1.2.643.6.57.1.1.1.1
( )	[TLS Client] Узел Мастерчейн	1.2.643.6.57.1.1.1.2
( )	[TLS Server] API узла Мастерчейн	1.2.643.6.57.1.1.1.3
( )	[TLS Server] API СПКС	1.2.643.6.57.1.2.1.1
( )	[TLS Client] API СПКС	1.2.643.6.57.1.2.1.2
( )	[TLS Client] АРМ Администратора Мастерчейн	1.2.643.6.57.1.3.1.3
( )	[TLS Server] API Системы мониторинга	1.2.643.6.57.1.4.1.1
( )	[TLS Client] API Системы мониторинга	1.2.643.6.57.1.4.1.2
( )	[TLS Client] АРМ Системы мониторинга	1.2.643.6.57.1.4.1.3
( )	[TLS Server] API ИС	1.2.643.6.57.1.5.1.1
( )	[TLS Client] API ИС	1.2.643.6.57.1.5.1.2
( )	[TLS Client] АРМ ИС	1.2.643.6.57.1.5.1.3
( )	[Sign] Админ сети	1.2.643.6.57.1.3.2.1
( )	[Sign] Админ Whitelist	1.2.643.6.57.1.3.2.2
( )	[Sign] АРМ Мониторинга Мастерчейн	1.2.643.6.57.1.4.2.1
( )	[Sign] АРМ Мониторинга Мастерчейн Участник	1.2.643.6.57.1.4.2.2
( )	[Sign] АРМ ИС Админ	1.2.643.6.57.1.5.2.1
( )	[Sign] АРМ ИС робот	1.2.643.6.57.1.5.2.2
( )	[Sign] АРМ ИС Админ Банка	1.2.643.6.57.1.5.2.3
( )	[Sign] АРМ ИС Менеджер Банка	1.2.643.6.57.1.5.2.4

( )	[Sign] CMS Storage	1.2.643.6.57.1.2.2.1
( )	[Block Sign] Узел Мастерчейн	1.2.643.6.57.1.1.3.1
( )	[Encrypt Payload] CMS Storage Transport Key	1.2.643.6.57.1.2.4.1
( )	[Encrypt Payload] CMS IS Transport Key	1.2.643.6.57.1.2.4.2
( )	[Encrypt Payload] CMS IS User Transport Key	1.2.643.6.57.1.2.4.3
( )	[TLS Server] Узел Мастерчейн (ДДС 2.0)	1.2.643.6.57.1.2.1.1.1
( )	[TLS Client] Узел Мастерчейн (ДДС 2.0)	1.2.643.6.57.1.2.1.1.2
( )	[TLS Server] API узла Мастерчейн (ДДС 2.0)	1.2.643.6.57.1.2.1.1.3
( )	[TLS Server] API ИС (ДДС 2.0)	1.2.643.6.57.1.2.5.1.1
( )	[TLS Client] API ИС (ДДС 2.0)	1.2.643.6.57.1.2.5.1.2
( )	[TLS Client] АРМ ИС (ДДС 2.0)	1.2.643.6.57.1.2.5.1.3
( )	[TLS Server] API СПКС (ДДС 2.0)	1.2.643.6.57.1.2.2.1.1
( )	[TLS Client] API СПКС (ДДС 2.0)	1.2.643.6.57.1.2.2.1.2
( )	[Sign] АРМ ИС Робот (ДДС 2.0)	1.2.643.6.57.1.2.5.2.2
( )	[Sign] АРМ ИС Админ Банка (ДДС 2.0)	1.2.643.6.57.1.2.5.2.3
( )	[Sign] АРМ ИС Менеджер Банка (ДДС 2.0)	1.2.643.6.57.1.2.5.2.4
( )	[Sign] CMS Storage (ДДС 2.0)	1.2.643.6.57.1.2.2.2.1
( )	[Encrypt Payload] CMS IS (ДДС 2.0)	1.2.643.6.57.1.2.2.4.1
( )	[Encrypt Payload] CMS IS API Transport Key (ДДС 2.0)	1.2.643.6.57.1.2.2.4.2
( )	[Encrypt Payload] CMS IS User Transport Key (ДДС 2.0)	1.2.643.6.57.1.2.2.4.3
( )	[Block Sign] Узел Мастерчейн (ДДС 2.0)	1.2.643.6.57.1.2.1.3.1

( ) В заявлении допускается отмечать только одно значение из множества!

Примечание: * - установить указатель в одно из указанных положений

Должность и Ф.И.О. лица, уполномоченного совершать сделки, направленные на приобретение услуг Удостоверяющего центра ООО «Крипто-Про».

_____/_____/

М.П.

Владелец ЭП _____/_____/

« »_____202____

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

Заявление на аннулирование/прекращение действия (отзыв) сертификата ключа проверки электронной 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/прекратить действие (отозвать) сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО», содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Общее имя
INN	ИНН организации
OGRN	ОГРН организации
SurName (SN)	Фамилия полномочного представителя, действующего от имени организации
GivenName (GN)	Имя и Отчество уполномоченного представителя

Должность и Ф.И.О. лица, уполномоченного совершать сделки, направленные на приобретение услуг Удостоверяющего центра ООО «Крипто-Про» и подписывать документы.

_____/_____/

"___" _____ 20__ г.

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

Заявление на приостановление действия сертификата ключа проверки электронной 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 своего сертификата ключа проверки электронной подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Общее имя
INN	ИНН организации
OGRN	ОГРН организации
SurName (SN)	Фамилия полномочного представителя, действующего от имени организации
GivenName (GN)	Имя и Отчество уполномоченного представителя

Срок приостановления действия сертификата ключа проверки электронной подписи _____ дней.
(количество дней прописью)

Должность и Ф.И.О. лица, уполномоченного совершать сделки, направленные на приобретение услуг Удостоверяющего центра ООО «Крипто-Про» и подписывать документы.

_____/_____/
«____» _____ 20____ г.

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

Заявление на возобновление действия сертификата ключа проверки электронной 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 своего сертификата ключа проверки электронной подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Общее имя
INN	ИНН организации
OGRN	ОГРН организации
SurName (SN)	Фамилия полномочного представителя, действующего от имени организации
GivenName (GN)	Имя и Отчество уполномоченного представителя

Должность и Ф.И.О. лица, уполномоченного совершать сделки, направленные на приобретение услуг Удостоверяющего центра ООО «Крипто-Про» и подписывать документы.

_____/_____/

«____» _____ 20____ г.

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

Для юридических лиц

Заявление на получение информации о статусе
сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО»

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит предоставить информацию о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «КРИПТО-ПРО» и содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Наименование организации, если владелец сертификата – юридическое лицо; Фамилия, Имя, Отчество, если владелец сертификата – физическое лицо

Время (период времени) на момент наступления которого требуется установить статус сертификата: с «____» по «_____».

Должность и Ф.И.О. лица, уполномоченного совершать сделки, направленные на приобретение услуг Удостоверяющего центра ООО «Крипто-Про» и подписывать документы.

_____/_____/

«____» _____ 20____ г.

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

Для юридических лиц

Заявление на проверку подлинности электронной подписи в электронном документе

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

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит проверить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–XXX;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № Н–XXX
3. Время[1] подписания электронной подписью электронного документа:
«_____:_____» «___/_____/_____»;
Час минута день месяц год
Если момент подписания электронного документа не определен, то указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:
«_____:_____» «___/_____/_____»;
Час минута день месяц год

Должность и Ф.И.О. лица, уполномоченного совершать сделки, направленные на приобретение услуг Удостоверяющего центра ООО «Крипто-Про» и подписывать документы.

_____/_____/

«____» _____ 20____ г.

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

Копия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (Пример)

Сведения о сертификате:
Этот сертификат:
Подтверждает удаленному компьютеру идентификацию вашего компьютера
Защищает сообщения электронной почты
Кому выдан:
Фамилия Имя Отчество
Кем выдан:
CryptoPro CA
Действителен с 15 октября 2013 г. 12:03:00 UTC по 15 октября 2014 г. 12:12:00 UTC
Версия: 3 (0x2)
Серийный номер: 14F5 9CF2 0000 0000 003A
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2012
Идентификатор: 1.2.643.2.2.3
Параметры: 0500
Издатель сертификата: CN = CryptoPro CA, C = RU
Срок действия:
Действителен с: 15 октября 2013 г. 12:03:00 UTC
Действителен по: 15 октября 2014 г. 12:12:00 UTC
Владелец сертификата: CN = User1
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-12
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: Электронная 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) 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 34.11/34.10-2012
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.

Подпись владельца сертификата ключа проверки электронной подписи:

_____/_____

"___" _____ 20__ г.

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

Перечень
автоматизированных систем, в отношении которых ООО «Системы распределенного реестра» выполняет функции администратора автоматизированной системы

1. СКЗИ «Мастерчейн»
2. Автоматизированная система «программный комплекс «Децентрализованная депозитарная система»».
3. Автоматизированная система «программный комплекс «Цифровые банковские гарантии»».