Утверждаю
Генеральный директор
ООО «КриптоСтандарт»

_____/Е.В. Морозов/
Приказ № 3 от «23» января 2017г.

Регламент Удостоверяющего Центра ООО «КриптоСтандарт»

г.Ростов-на-Дону
2017

Содержание

1. Общие положения.....3
1.1. Сведения об Удостоверяющем центре.....3
1.2.Термины и определения.....4
1.3.Предмет регулирования Регламента.....6
2.Деятельность Удостоверяющего центра.....7
3. Права и обязанности сторон.....8
3.1. Обязанности Удостоверяющего центра.....8
3.2. Обязанности Пользователя Удостоверяющего центра.....9
3.3. Права Удостоверяющего центра.....9
3.4. Права Пользователя Удостоверяющего центра.....10
4. Ответственность сторон.....10
5. Обеспечительные процедуры.....11
5.1.Предоставление информации и документов.....11
5.2.Смена ключа Уполномоченного лица Удостоверяющего центра.....11
5.3.Смена ключа электронной подписи Пользователя Удостоверяющего центра.....12
6.Порядок предоставления и пользования услугами Удостоверяющего центра.....13
6.1. Изготовление сертификата ключа подписи.....13
6.2.Прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра.....13
6.3. Получение информации о статусе сертификата ключа подписи.....14
6.4. Подтверждение подлинности электронной цифровой подписи в электронном документе.....14
6.5. Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени.....15
6.6.Форма сертификата ключа проверки электронной подписи и списка отозванных сертификатов.....16
7. Иные положения.....17
7.1.Сроки действия ключей электронной подписи и сертификатов ключей проверки электронной подписи.....17
7.2.Политика конфиденциальности.....18
7.3.Форс-мажор.....18
7.4.Разрешение споров.....19
7.5.Архивное хранение документированной информации.....19
7.6.Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.....20
8. Список приложений.....20

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1.Сведения об Удостоверяющем центре.

Удостоверяющий центр – организация, осуществляющая функции по созданию и выдаче сертификатов ключей проверки электронных подписей и иные функции удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ).

ООО «КриптоСтандарт» является аккредитованным Минкомсвязи России удостоверяющим центром (Свидетельство об аккредитации удостоверяющего центра №09 от 29 июня 2012 года) и осуществляет свою деятельность на территории Российской Федерации на основании лицензии № 3536 от 2 декабря 2014г., выданной УФСБ России по Ростовской области, на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание 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).

Полное наименование организации: Общество с ограниченной ответственностью «КриптоСтандарт».
Юридический адрес: 344002, г. Ростов-на-Дону, пер. Малый,19**.**
Фактический адрес: 344002, г. Ростов-на-Дону, пер. Малый,19.
ИНН/КПП: 6163100972/616301001
Р/сч: 30101810160150000063, ФИЛИАЛ "ЮЖНЫЙ" БАНКА ВТБ (ПАО), БИК 046015063
Корр/сч: 30101810900000000991
ОГРН 1106195001494
ИНН/КПП: 6163100972/616301001
Телефон:(863) 333-22-86
E-mail: info@cryptostandart.ru.

Обособленное подразделение в г.Каменск-Шахтинский

Адрес	347810, Ростовская область, г. Каменск-Шахтинский, пр-кт Карла Маркса,18
Телефоны	(86365) 7-20-88, 8928-118-28-90
Email	kamensk@cryptostandart.ru

Обособленное подразделение в г.Волгодонск

Адрес	347375, Ростовская область, г. Волгодонск, ул. Ленинградская, 10, оф.104
Телефоны	(8639) 245-045, 230-424

Email	volgodonsk@cryptostandart.ru

Обособленное подразделение в г.Зерноград

Адрес	Ростовская область, г. Зерноград, ул. Березовая, 4а, офис 50
Телефоны	(863)322-03-32
Email	zernograd@cryptostandart.ru

Обособленное подразделение в г.Ялта

Адрес	298600, Республика Крым, г. Ялта, ул. Васильева, 16, оф. 401
Телефоны	8-800-777-23-05
Email	yalta@cryptostandart.ru

1.2.Термины и определения.

Администратор Удостоверяющего центра – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей подписей Пользователей Удостоверяющего центра и уполномоченный Удостоверяющим центром расписываться собственноручной подписью в сертификатах ключей подписей на бумажном носителе, изданных Удостоверяющим центром.

Аутентификация - Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

Заявитель − юридическое лицо независимо от организационно-правовой формы, физическое лицо или иной хозяйствующий субъект (в том числе индивидуальный предпри-ниматель, адвокат, нотариус и т.д.), обращающиеся в Удостоверяющий центр для получения Сертификата и заключившие соответствующий договор с Удостоверяющим центром. После создания Сертификата Заявитель становится Владельцем сертификата

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано**.**

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

Клиент – юридическое или физическое лицо, пользующееся услугами другого физического или юридического лица, вступающее с ним в деловые отношения, оформленные письменным договором.

Ключевой носитель – внешнее (съемное) устройство, используемое для хранения ключевых контейнеров с закрытыми (секретными) ключами. Один ключевой носитель может содержать один или несколько ключевых контейнеров с различными ключами.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

Корпоративная информационная система - информационная система, участни-ками которой может быть ограниченный круг лиц, определенный ее оператором или согла-шением участников этой информационной системы.

Оператор Службы актуальных статусов сертификатов - ответственный сотрудник Удостоверяющего центра, являющийся владельцем сертификата ключа подписи и соответствующего закрытого ключа, с использованием которого подписываются электронной цифровой подписью электронные ответы Службы актуальных статусов сертификатов.

Оператор Службы штампов времени - ответственный сотрудник Удостоверяющего центра, являющийся владельцем сертификата ключа подписи и соответствующего закрытого ключа, с использованием которого подписываются электронной цифровой подписью штампы времени.

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

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 09:00 по 18:00 (по Московскому времени) каждого дня недели за исключением выходных и праздничных дней.

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Список отозванных сертификатов (СОС) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на определенный момент времени были аннулированы или действие которых было приостановлено.

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

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей проверки электронных подписей и списков отозванных сертификатов.

Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме органы государственной власти или органы местного самоуправления (далее – органы власти), юридические и физические лица

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

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Электронный документ – документ, информация в котором представлена в электронно-цифровой форме.

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

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 осуществляет свою работу в соответствии со следующими стандартами PKCS:

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные;
- PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи.

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

1.3.Предмет регулирования Регламента

1.3.1.Регламент оказания услуг Удостоверяющего центра (далее - Регламент) - документ, определяющий условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Удостоверяющего центра. Настоящий Регламент определяет механизмы и условия предоставления и использования услуг Общества с ограниченной ответственностью «КриптоСтандарт» (ООО «КриптоСтандарт»), далее по тексту - Удостоверяющий центр или Центр, в сфере правоотношений, возникающих в рамках действия Федерального закона от 06.04.2011г.N-63ФЗ «Об электронной подписи», а также иных нормативно-правовых актов действующего законодательства РФ, регулирующих вышеуказанный вид правоотношений.

Регламент Удостоверяющего центра ООО «КриптоСтандарт», именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

Любое заинтересованное лицо может ознакомиться с Регламентом, обратившись к ресурсу сайта Удостоверяющего центра по адресу www.cryptostandart.ru.

1.3.2.*Субъекты, на которых распространяет свое действие настоящий Регламент*.

Субъекты - это все лица, которые в силу настоящего Регламента, договора или действующего законодательства обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Регламентом. Субъектами являются – Заявитель, Участники электронного взаимодействия, Владелец сертификата, Удостоверяющий центр.

1.3.3. *Порядок присоединения к Регламенту*.

Лицо, заключившее с Удостоверяющим центром договор, предусматривающий выдачу Сертификатов, а также лицо, подавшее заявление на выдачу Сертификата, присоединяется к настоящему Регламенту в силу статьи 428 Гражданского кодекса Российской Федерации и обязано соблюдать его требования.

Владелец сертификата имеет право в одностороннем порядке прекратить взаимодействие с Удостоверяющим центром в рамках Регламента, направив в Удостоверяющий центр заявление на прекращение действия выданного ему Сертификата.

1.3.4. *Изменения (дополнения) Регламента.*

Все изменения (дополнения) в Регламент, включая приложения к нему, производятся Удостоверяющим центром в одностороннем порядке. Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного

размещения указанных изменений (дополнений) на сайте Удостоверяющего центра по адресу - www.cryptostandart.ru.

Внесенные изменения вступают в силу и становятся обязательными для участников договорных отношений по истечении 10 (десяти) календарных дней с момента даты опубликования нового Регламента на сайте Удостоверяющего центра.

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

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

1.3.5. Информирование субъектов.

Информирование субъектов Удостоверяющим центром может производиться посредством: направления электронного письма на адрес, указанный при обращении и/или ином взаимодействии с Удостоверяющим центром, направления SMS-уведомлений на телефонный номер, представленный Заявителем в Удостоверяющий центр, ответа на телефонный звонок и/или посредством размещения информации на сайте по адресу www.cryptostandart.ru.

1.3.6. Вознаграждение Удостоверяющего центра

- Удостоверяющий центр осуществляет свою деятельность на платной основе.
- Стоимость и состав услуг Удостоверяющего центра определяются прайс-листом, который публикуется на сайте www.cryptostandart.ru .
- Сроки и порядок расчетов за услуги, оказываемые Удостоверяющим центром, регулируются условиями договоров между Удостоверяющим центром и Заявителем.

2.ДЕЯТЕЛЬНОСТЬ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.

В процессе своей деятельности Удостоверяющий центр :

1)создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата.

2)устанавливает сроки действия сертификатов ключей проверки электронных подписей;

3) аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей;

4) выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

5) ведет реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях прекращения или аннулированиясертификатов;

6) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

7) создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

8) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

9) осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

10) осуществляет иную деятельность.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН.

3.1. Обязанности Удостоверяющего центра.

Удостоверяющий центр обязан:

- отказать в изготовлении ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи в следующих случаях:

1. представление не надлежащим образом оформленных документов;
2. противоречия сведений, указанных в предоставленных документах;
3. не предоставление необходимого комплекта документов;
4. отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи;
5. не подтверждение того, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи.

-вносить в создаваемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами;

- использовать для изготовления ключа электронной подписи уполномоченного лица Удостоверяющего центра и формирования электронной подписи, только сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи;

- использовать ключ электронной подписи уполномоченного лица Удостоверяющего центра только для подписи издаваемых им сертификатов ключей проверки электронной подписи и списков отозванных сертификатов;

- принять меры по защите ключа электронной подписи уполномоченного лица Удостоверяющего центра от несанкционированного доступа;

- организовать свою работу по GMT (Greenwich Mean Time) с учетом московского часового пояса. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности;

- обеспечить регистрацию пользователей в Удостоверяющем центре в соответствии с порядком, определенным в настоящем Регламенте;

- обеспечить занесение регистрационной информации Пользователя Удостоверяющего центра в Реестр Удостоверяющего центра и обеспечить уникальность регистрационной информации всех зарегистрированных в Удостоверяющем центре лиц, используемой для идентификации владельцев сертификатов ключей проверки электронной подписи;

- в соответствии с ч.5 ст.18 ФЗ «Об электронной подписи» направлять в единую систему идентификации и аутентификации сведения о лице, получившем сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат), в объеме, необходимом для регистрации в единой системе идентификации и аутентификации;

- изготовить сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявке на изготовление сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте;

- обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей проверки электронной подписи;

- обеспечить уникальность значений открытых ключей в изготовленных сертификатах ключей проверки электронной подписи пользователей Удостоверяющего центра;

- обеспечить сохранение в тайне изготовленного ключа электронной подписи Пользователя Удостоверяющего центра;

- прекратить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по соответствующему заявлению на прекращение действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем «Регламенте;

– публиковать актуальный список отозванных сертификатов на сайте Удостоверяющего центра в ресурсе: www.cryptostandart.ru. Период публикации списка отозванных сертификатов Удостоверяющего центра - 12 часов.

3.2. Обязанности Пользователя Удостоверяющего центра.

Пользователь, присоединившийся к «Регламенту» обязан:

- известить Удостоверяющий центр об изменениях в документах, указанных в разделе 3 данного регламента и предоставить их в течение 3 (трех) рабочих дней с момента регистрации таких изменений;

- обращаться не реже одного раза в тридцать календарных дней на сайт Удостоверяющего центра по адресу www.cryptostandart.ru за сведениями об изменениях и дополнениях в Регламент;

- хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования;

- применять для формирования электронной подписи, только действующий ключ электронной подписи;

- не применять ключ электронной подписи, если стало известно, что этот ключ несанкционированно используется или использовался ранее другими лицами;

– немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата ключа проверки электронной подписи в случае потери, компрометации, искажения ключей электронной подписи.

3.3. Права Удостоверяющего центра.

Удостоверяющий центр имеет право:

-запрашивать у заявителя документы для подтверждения информации, содержащейся в заявлении на создание и выдачу сертификата;

- отказать в изготовлении сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по основаниям, предусмотренным настоящим Регламентом и законодательством РФ;

- не принимать от заявителя документы, не соответствующие требованиям действующих нормативных правовых актов РФ;

-отказать владельцу сертификата в прекращении действия сертификата в случае, если сертификат уже аннулирован или прекратил свое действие по другим основаниям;

- отказать в предоставлении сведений, содержащихся в реестре выданных сертификатов, в случае, если объём запрашиваемых данных не соответствует законной цели обработки этих данных, заявленной в запросе на предоставление сведений;

- использовать представленные Заявителем номера мобильной связи и адреса электронной почты для рассылки уведомлений об окончании срока действия Сертификата, предоставлении услуг Удостоверяющего центра.

– в одностороннем порядке аннулировать действие сертификата ключа проверки электронной подписи в случаях, установленных Федеральным законом от 06.04.2011г.N-63ФЗ «Об электронной подписи», иным законодательством РФ.

3.4. Права Пользователя Удостоверяющего центра.

Пользователь Удостоверяющего центра имеет право:

- применять сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра для проверки электронной подписи уполномоченного лица Удостоверяющего центра в сертификатах ключей проверки электронной подписи, изготовленных Удостоверяющим центром;
- применять список отозванных сертификатов ключей подписей, изготовленный Удостоверяющим центром, для установления статуса сертификатов ключей проверки электронной подписи, изготовленных Удостоверяющим центром;
- применять сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи;
- для хранения ключа электронной подписи применять сертифицированный носитель, поддерживаемый средством электронной подписи и Удостоверяющим центром;
- обратиться в Удостоверяющий центр с заявлением на изготовление сертификата ключа проверки электронной подписи;
- обратиться в Удостоверяющий центр за получением информации о статусе сертификатов ключей проверки электронной подписи и их действительности на определенный момент времени;

– обратиться в Удостоверяющий центр за подтверждением подлинности электронной подписи в электронном документе, сформированной с использованием сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром.

4. ОТВЕТСТВЕННОСТЬ СТОРОН

4.1. Ответственность Удостоверяющего центра определяется действующим законодательством РФ (в т.ч. ст.16 №63-ФЗ «Об электронной подписи»).

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

- если Удостоверяющий центр обоснованно полагался на сведения, представленные Заявителем;
- подделки, подлога либо иного искажения Заявителем, Владельцем сертификата либо третьими лицами информации, содержащейся в заявлении либо иных документах, представленных в Удостоверяющий центр.

4.3. Удостоверяющий центр не несет ответственность за невозможность использования Сертификата в случае, если такая невозможность возникла после создания Сертификата и вызвана изменением требований информационных систем или действующих нормативно-правовых актов.

4.4 Ответственность Субъектов, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

4.5. Для изготовления ключа электронной подписи и сертификата проверки ключа электронной подписи Центр использует ключевые носители, имеющие сертификат соответствия (по требованиям безопастности информации № РОСС RU.0001.01БИ 00), в т.ч.:программно-аппаратный комплекс «Интеллектуальный ключевой носитель информации «Rutoken lite», программно-аппаратный комплекс аутентификации и хранения ключевой ниформации пользователей «Электронный ключ eToken 5», программно-аппаратный комплекс аутентификации и безовасного хранения информации пользователей Jacarta». Гарантийный срок

эксплуатации ключевых носителей составляет 1 (один) год. В случае невозможности эксплуатации ключевого носителя, произошедшего не по вине Пользователя, Удостоверяющий центр заменяет ключевой носитель.

5. ОБЕСПЕЧИТЕЛЬНЫЕ ПРОЦЕДУРЫ

5.1.Представление информации и документов

5.1.1. Заявитель представляет в Удостоверяющий центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности Заявителя, Уполномоченного представителя Заявителя, Заявителя-физического лица, а также документы, на основании которых Удостоверяющим центром вносятся сведения в Сертификат, такие как: полное или сокращенное наименование, основной государственный регистрационный номер, юридический адрес, идентификационный номер налогоплательщика, код причины постановки на учет, страховой номер индивидуального лицевого счета, наименование должности и иные данные.
5.1.2. Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность – паспорту гражданина РФ. В исключительных случаях отсутствия у гражданина РФ основного документа, удостоверяющего личность, Удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность, признаваемому таковым действующим законодательством.
5.1.3. Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства, признаваемому таковым действующим законодательством.
5.1.4. Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, признаваемого действующим законодательством в качестве удостоверяющего личность данных категорий лиц.
5.1.5. При обращении в Удостоверяющий центр Уполномоченного представителя Заявителя его полномочия должны быть подтверждены соответствующей доверенностью.
5.1.6. Надлежащим способом заверения копий документов может являться нотариальное заверение копий, заверение копий органом власти (например, налоговыми органами), заверение копий документов Заявителем самостоятельно.
5.1.7. Нотариально заверенные копии документов должны содержать штамп нотариуса «копия верна», штамп с информацией о нотариусе, должны быть заверены печатью нотариуса и иметь подпись нотариуса.
5.1.8. Копии, заверенные Заявителем, могут предоставлять исключительно юридические лица и индивидуальные предприниматели, имеющие собственную печать. Многостраничные копии либо должны быть прошиты и заверены на листе сшивки, либо заверены на каждой странице (подпись руководителя организации и печать организации).
5.1.9. Копии документов, заверенные органом власти, должны содержать подпись и расшифровку подписи должностного лица, их заверившего, а также печать/штамп данного органа власти.
5.1.10 К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.
5.1.11. Документы и их надлежащим образом заверенные копии, представленные в Удостоверяющий центр для целей выдачи Сертификата, остаются на хранении в Удостоверяющем центре и возврату не подлежат.

5.2. Смена ключа электронной подписи Уполномоченного лица Удостоверяющего центра.

5.2.1. Плановая смена ключа электронной подписи уполномоченного лица Удостоверяющего центра.

Плановая смена ключа электронной подписи Уполномоченного лица Удостоверяющего центра выполняется в период действия ключа электронной подписи Уполномоченного лица Удостоверяющего центра. Процедура плановой смены ключа электронной подписи уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:
- Уполномоченное лицо Удостоверяющего центра генерирует новый ключ электронной подписи;
- Уполномоченное лицо Удостоверяющего центра изготавливает новый сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра.

Уведомление пользователей о проведении смены ключа уполномоченного лица Удостоверяющего центра осуществляется посредством размещения информации на сайте www.cryptostandart.ru.

Старый 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 ключа электронной подписи уполномоченного лица Удостоверяющего центра.

5.2.2. Внеплановая смена ключа электронной подписи уполномоченного лица Удостоверяющего центра.

Внеплановая смена ключа выполняется в случае компрометации или угрозы компрометации ключа электронной подписи Уполномоченного лица Удостоверяющего центра.

В случае компрометации или угрозы компрометации ключа электронной подписи Уполномоченного лица Удостоверяющего центра сертификат Уполномоченного лица Удостоверяющего центра прекращает свое действие, Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте или публикации информации о компрометации на сайте Удостоверяющего центра. Все сертификаты, подписанные с использованием скомпрометированного ключа электронной подписи уполномоченного лица Удостоверяющего центра, считаются прекратившими свое действие.

После прекращения действия сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены ключа электронной подписи уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключа электронной подписи уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица Удостоверяющего центра.

Все действовавшие на момент компрометации ключа электронной подписи Уполномоченного лица Удостоверяющего центра сертификаты ключей проверки электронной подписи, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

5.3. Смена ключа электронной подписи Пользователя Удостоверяющего центра.

5.3.1. Плановая смена ключа электронной подписи пользователя Удостоверяющего центра.

Плановая смена ключа электронной подписи пользователя происходит по заявке Пользователя. Изготовление ключа проверки электронной подписи осуществляется в соответствии с настоящим Регламентом.

5.3.2. Внеплановая смена ключа электронной подписи пользователя Удостоверяющего центра**.**

Пользователь УЦ самостоятельно принимает решение о факте или угрозе компрометации своего ключа электронной подписи.

В случае компрометации или угрозы компрометации ключа электронной подписи Пользователь УЦ предоставляет Администратору Удостоверяющего центра заявление на прекращение действия сертификата, после чего осуществляется изготовление ключа электронной подписи (в соответствии с настоящим Регламентом).

6.ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.

6.1. Изготовление сертификата ключа проверки электронной подписи.

Удостоверяющий центр осуществляет изготовление сертификатов ключей проверки электронной подписи физическим и юридическим лицам только в случае их «присоединения» к Регламенту.

Удостоверяющий центр согласует с юридическим или физическим лицом дату выполнения работ по созданию сертификатов ключей проверки электронной подписи.

В соответствии с согласованной датой работ, владельцы сертификатов ключей проверки электронной подписи, указанные в заявке пользователя, лично или их доверенные лица, прибывают в офис Удостоверяющего центра, где:

- получают изготовленные в их присутствии ключи и сертификаты ключей проверки электронной подписи;
- подписывают акт о получении ключей электронной подписи и сертификатов ключей проверки электронной подписи;
- расписываются в бланках сертификатах ключей проверки электронной подписи на бумажном носителе;
-получают ключевую фразу для связи на случай компрометации ключей;
- получают инструктаж по правилам работы с СКЗИ, криптографическими ключами и сертификатами ключа проверки электронной подписи.

6.2. Прекращение (аннулирование) действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра**.**

Сертификат ключа проверки электронной подписи прекращает свое действие:

1) в связи с истечением установленного срока его действия;

2) на основании заявления владельца сертификата ключа проверки электронной подписи. Подача заявления на прекращение действия сертификата ключа проверки электронной подписи осуществляется Пользователем Удостоверяющего центра посредством почтовой или курьерской связи по форме Приложения № 1.

3) в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;

4) в иных случаях, установленных Федеральным законом от 06.04.2011г.N-63ФЗ «Об электронной подписи», принимаемыми в соответствии с ними нормативными правовыми актами, или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

1) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

2) установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;

3) вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

После получения Удостоверяющим центром заявления на прекращение действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра осуществляет его

рассмотрение и обработку. Обработка заявления на прекращение действия сертификата должна быть осуществлена в течение 30 минут с момента получения заявления.

В случае отказа в прекращении действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом Пользователя Удостоверяющего центра.

В случае положительного решения Администратора Удостоверяющего центра по заявлению владельца сертификата на прекращение действия сертификата или вступления в силу решения суда, или поступления других оснований досрочного прекращения действия (аннулирования) сертификата Удостоверяющий центр в течение 30 минут вносит информацию об этом в реестр сертификатов и публикует обновленный список отозванных сертификатов. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестре сертификатов.

6.3. Получение информации о статусе сертификата ключа проверки электронной подписи.

Получение информации о статусе сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром осуществляется на основании заявления Пользователя Удостоверяющего центра. Данное заявление оформляется по форме Приложения № 2 настоящего Регламента и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

- время и дата подачи заявления;
- время и дата (либо период времени), на момент наступления, которых требуется установить статус сертификата ключа проверки электронной подписи;
- идентификационные данные владельца сертификата ключа проверки электронной подписи, статус которого необходимо установить;
- серийный номер сертификата ключа проверки электронной подписи, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата ключа проверки электронной подписи, которая предоставляется Пользователю Удостоверяющего центра.

6.4. Подтверждение подлинности электронной подписи в электронном документе.

По желанию Пользователя УЦ, Удостоверяющий центр осуществляет проведение экспертных работ по подтверждению подлинности электронной подписи в электронном документе.

В данном случае для подтверждения подлинности электронной подписи в электронных документах Пользователь УЦ подает заявление в Удостоверяющий центр по форме, приведенной в Приложении №3.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность электронной подписи которого необходимо подтвердить в электронном документе;
- время и дата формирования электронной подписи электронного документа;
- время и дата, на момент наступления, которых требуется установить подлинность электронной подписи.

Обязательным приложением к заявлению на подтверждение подлинности электронной подписи в электронном документе является внешний носитель, содержащий:

- сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе (в виде файла стандарта CMS);
- электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

Если формат представления электронной подписи (формат представления электронного документа с электронной подписью) соответствует стандарту криптографических сообщений (CMS), то Удостоверяющий центр обеспечивает проверку подлинности электронной подписи в электронном документе. Решение о соответствии формата представления электронной подписи (формата представления электронного документа с электронной подписью) стандарту CMS принимает Удостоверяющий центр.

Проведение работ по подтверждению подлинности электронной подписи в электронном документе осуществляет Администратор Удостоверяющего центра.

Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается Администратором и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по подтверждению подлинности электронной подписи в одном электронном документе и предоставлению пользователю заключения по выполненной проверке составляет пять рабочих дней с момента поступления заявления в Удостоверяющий центр.

6.5.Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени**.**

Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе сертификатов ключей проверки электронной подписи посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам Пользователей Удостоверяющего центра формирует и предоставляет этим пользователям OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра. OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- Выполнены условия признания квалифицированной электронной подписи в OCSP-ответе.
- Квалифицированная электронная подпись в OCSP-ответе сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Службы актуальных статусов сертификатов, а именно: сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов в расширении Extended Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.9 – «Подпись ответа службы OCSP».

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра – http://top.cryptostandart.ru/ocsp/ocsp.srf. Указанный адрес заносится в расширение Authority Information Access (AIA) создаваемых Удостоверяющим центров сертификатов ключей проверки электронной подписи.

Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени. Штамп времени, относящийся к подписанному электронной подписью электронному документу, признается действительным при одновременном выполнении следующих условий:

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

Адрес обращения к Службе штампов времени Удостоверяющего центра – http://top.cryptostandart.ru/tsp/tsp.srf.

6.6.Форма сертификата ключа проверки электронной подписи и списка отозванных сертификатов.

Форма сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром.

Форма сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Форма списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	**Описание**	**Содержание**
Version	Версия	V2
Issuer	Издатель СОС	Идентифицирующие данные Уполномоченного лица УЦ
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	ЭЦП издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор версии сертификата	Версия сертификата Уполномоченного лица Удостоверяющего центра

7. ИНЫЕ ПОЛОЖЕНИЯ

7.1.Сроки действия ключей электронной подписи и сертификатов ключей проверки электронной подписи.

7.1.1. Срок действия ключа электронной подписи и сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра.

Срок действия 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 ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи уполномоченного лица Удостоверяющего центра исчисляется с даты и времени генерации ключа электронной подписи 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 подписи Уполномоченного лица Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

7.1.2. Срок действия ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя УЦ.

Срок действия ключа электронной подписи Пользователя УЦ составляет 1 (Один) год.

Начало периода действия ключа электронной подписи Пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

Срок действия сертификата ключа проверки электронной подписи Пользователя УЦ не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Пользователя УЦ и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

7.1.3. Срок действия ключа электронной подписи и сертификата ключа проверки электронной подписи Служб Удостоверяющего центра.

Срок действия ключа электронной подписи Службы актуальных статусов сертификатов составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи Службы актуальных статусов сертификатов исчисляется с даты и времени создания сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов.

Срок действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

Срок действия ключа электронной подписи Службы штампов времени составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи Службы штампов времени исчисляется с даты и времени создания сертификата ключа проверки электронной подписи Службы штампов времени.

Срок действия сертификата ключа проверки электронной подписи Службы штампов времени не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы штампов времени и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

7.2. Политика конфиденциальности.

Удостоверяющий центр выделяет следующие типы конфиденциальной информации и порядок обращения с ней:

- Ключ электронной подписи владельца. Удостоверяющий центр не копирует ключи электронной подписи Клиентов.

-Пароль доступа к контейнеру, содержащему ключи электронной подписи, сообщается только владельцу, на чье имя выпущен соответствующий ключу электронной подписи сертификат. Либо передается лицу, на чье имя выдана доверенность на получения такой информации.

-Персональная и корпоративная информация Клиентов (пользователей услуг) не подлежащая внесению в содержание электронного сертификата и в состав списка отозванных сертификатов. Эта информация не подлежит разглашению.

-Информация, хранящаяся в журналах аудита Удостоверяющего центра. Эта информация не подлежит разглашению.

-Отчетные материалы по выполненным проверкам деятельности Удостоверяющего центра. Эта информация не подлежит разглашению.

Удостоверяющий центр выделяет следующие типы не конфиденциальной информации – общедоступной информации:

- информация, включаемая в сертификаты открытых ключей пользователей;
- информация, включаемая в списки отозванных сертификатов;
- информация о настоящем регламенте.

Не конфиденциальная информация публикуется по решению Удостоверяющего центра. Место, способ и время публикации не конфиденциальной информации определяется самостоятельным решением Удостоверяющего центра и выполняется в соответствии с настоящим «Регламентом».

Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях и порядке, установленных законодательством РФ.

7.3 Форс-мажор.

Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по договорам, правоотношения по которым определяются настоящим Регламентом, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после «присоединения» стороны договора к настоящему Регламенту.

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 аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по вышеуказанным договорам.

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

Сторона, для которой создалась невозможность исполнения своих обязательств, 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.

7.4.Разрешение споров.

В случае возникновения споров в части оказания услуг Удостоверяющим центром сторонами споров считаются Удостоверяющий центр и владелец сертификата ключа проверки электронной подписи (физическое или юридическое лицо). В случае возникновения споров между владельцами сертификатов, являющимися Клиентами Удостоверяющего центра, в качестве независимого эксперта для разрешения спорных вопросов может быть привлечен Удостоверяющий центр.

Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

Сторона, получившая от другой Стороны претензию, обязана в течение 15 (пятнадцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде Ростовской области.

7.5.Архивное хранение документированной информации.

7.5.1. Состав архивируемых документов**.**

Архивированию подлежит следующая документированная информация:

- реестр сертификатов ключей проверки электронной подписи пользователей Удостоверяющего центра;
- сертификаты ключей проверки электронной подписи Уполномоченного лица Удостоверяющего центра;
- журналы аудита программно-аппаратных средств обеспечения деятельности Удостоверяющего центра;
- реестр пользователей, зарегистрированных в Удостоверяющем центре;
- заявления на изготовление сертификатов ключей проверки электронной подписи ключей пользователей Удостоверяющего центра;
- заявления на прекращения действия сертификата ключа проверки электронной подписи;
- заявления на приостановление действия сертификата ключа проверки электронной подписи;
- заявления на возобновление действия сертификата ключа проверки электронной подписи;
- служебные документы Удостоверяющего центра.
- копии документов на бумажном носителе, полученные для формирования сведений, внесенных в сертификат ключа проверки электронной подписи.

7.5.2. Источник комплектования архивного фонда Удостоверяющего центра.

Источником комплектования архивного фонда Удостоверяющего центра является отдел (служба) Удостоверяющего центра, обеспечивающий(ая) документирование.

7.5.3. Архивохранилище**.**

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

7.5.4. Уничтожение архивных документов.

Уничтожение архивных документов осуществляется по истечении срока архивного хранения согласно действующему законодательству РФ и нормативным документам, регламентирующим порядок хранения архивных документов.

7.6. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Владелец квалифицированного сертификата обязан:

1) не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
2) уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.
3) не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.
4) использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены).
5) использовать для создания и проверки электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с законодательство РФ.
6) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия.

Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.

8. СПИСОК ПРИЛОЖЕНИЙ.

8.1.Приложение №1 Форма заявления на прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КриптоСтандарт».
8.2. Приложение №2. Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром ООО «КриптоСтандарт».
8.3. Приложение №3. Форма заявления на подтверждение подлинности электронной подписи в электронном документе.

Приложение №1
к «Регламенту «Удостоверяющего центра ООО «КриптоСтандарт»
(Форма заявления на прекращение действия сертификата ключа проверки электронной подписи)

Заявление на прекращение действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «КриптоСтандарт»

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____,
(должность)
_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит прекратить действие сертификата ключа проверки электронной подписи содержащий следующий серийный номер:_____

Должность и ФИО руководителя организации _____

«____» _____ 20____ г.

м.п.

Приложение №2
к «Регламенту «Удостоверяющего центра ООО «КриптоСтандарт»
(Форма заявления на получение информации о статусе сертификата)

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром ООО «КриптоСтандарт»

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

в лице _____,
(должность руководителя)

_____,
(ФИО руководителя)

действующего на основании _____

Просит предоставить информацию о статусе следующего сертификата ключа подписи:

_____
(серийный номер сертификата)

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

(Время и дата должны быть указаны по Московскому времени. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром)

Должность и ФИО руководителя организации _____

«____» _____ 20____ г.

м.п.

Приложение №3
к «Регламенту «Удостоверяющего центра ООО «КриптоСтандарт»
(Форма заявления на подтверждение подлинности электронной подписи)

Заявление на подтверждение подлинности электронной подписи в электронном документе

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____,
(должность руководителя)
_____,
(фамилия, имя, отчество руководителя)
действующего на основании _____

Просит подтвердить подлинность электронной подписи в документе на основании следующих данных:

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в документе на прилагаемом к заявлению носителе – (указать наименование и номер носителя);

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 – (указать наименование и номер носителя).

3. Время на момент наступления, которого требуется подтвердить подлинность ЭП: «_____:_____» «_____/_____/_____»;
Час минута день месяц год

(Время и дата должны быть указаны по Московскому времени. Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром)

Должность и ФИО руководителя организации _____

«____» _____ 20____ г.

м.п.