

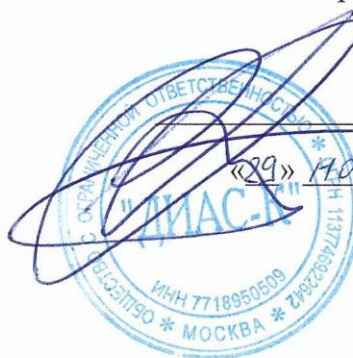
УТВЕРЖДАЮ

Генеральный директор

ООО «ДИАС-К»

/ Долинин Р.О./

«29» НОЯБРЯ 2018 года



**РЕГЛАМЕНТ**  
**оказания услуг удостоверяющего центра**  
**ООО «ДИАС-К»**

Москва 2018

## СОДЕРЖАНИЕ

1. Сведения об Удостоверяющем центре.....	3
2. Термины и определения .....	4
3. Общие положения .....	7
4. Вознаграждение Удостоверяющего центра .....	9
5. Представление информации и документов .....	10
6. Права и обязанности Субъектов .....	11
7. Ответственность субъектов .....	15
8. Порядок оказания услуг Удостоверяющего центра.....	166
9. Прочие условия .....	233
<b>Приложения.....</b>	<b>255</b>
Приложение № 1 к Регламенту Форма заявления на подтверждение ЭП Удостоверяющего центра в Сертификате .....	255
Приложение № 2 к Регламенту Форма заявления на подтверждение ЭП в электронном документе .....	266
Приложение № 3 к Регламенту Форма заявления на прекращение действия Сертификата.....	277
Приложение № 4 к Регламенту Форма заявления на изготовление квалифицированного сертификата.....	28
Приложение № 5 к Регламенту Форма доверенности на получение Сертификата .....	29
Приложение № 6 к Регламенту Расписка в получении Сертификата .....	30
Приложение №7 к Регламенту Профиль квалифицированного сертификата .....	31
Приложение № 8 к Регламенту УЦ ООО «ДИАС-К» РУКОВОДСТВО по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи .....	36

## 1. Сведения об Удостоверяющем центре

**Удостоверяющий центр** – подразделение ООО «ДИАС-К», осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей и иные функции удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ).

Удостоверяющий центр в качестве участника рынка услуг по созданию и выдаче сертификатов ключей проверки электронной подписей осуществляет свою деятельность на территории Российской Федерации на основании следующих документов:

– свидетельства об аккредитации удостоверяющего центра от 21.02.2017 рег. № 699;

– лицензии Центра по лицензированию, сертификации и защите государственной тайны Федеральной службы безопасности Российской Федерации от 18.04.2018 рег. № 16546Н на бланке ЛСЗ 0015283 на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию 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 и индивидуального предпринимателя).

Общество с ограниченной ответственностью «ДИАС-К», именуемое в дальнейшем **Удостоверяющий центр**, зарегистрировано на территории Российской Федерации в городе Москве.

**Юридический адрес** 107113, Москва г, Старослободская ул, 16/17

**Адрес Удостоверяющего центра:** 141143, Московская область, Щелковский район, сельское поселение Медвежье – Озерское, д. Медвежье Озера, ул. Сосновая, д. 11

**ИНН/КПП:** 7718950509/771801001

**Контактные телефоны, адрес электронной почты:**

**Тел.** +7-495-651-651-5

**e-mail:** [uc@diack.ru](mailto:uc@diack.ru)

**Время работы:**

по будням с 9 до 18 часов московского времени

## 2. Термины и определения

**21 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.

**22 Электронная подпись (далее – ЭП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

**23 Ключ электронной подписи (далее – Ключ ЭП)** – уникальная последовательность символов, предназначенная для создания электронной подписи.

**24 Ключ проверки электронной подписи (далее – Ключ проверки ЭП)** – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

**25 Простая электронная подпись (далее – ПЭП)** – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Для создания ПЭП используется ключ ПЭП – сочетание идентификатора и пароля (кода). Допустимые форматы ключа ПЭП, а также случаи и порядок использования ПЭП определяются настоящим Регламентом.

**26 Неквалифицированная электронная подпись (далее – НЭП)** – усиленная электронная подпись, соответствующая следующим признакам:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи и средств (средства) электронной подписи; позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
- позволяет определить лицо, подписавшее электронный документ;
- создается с использованием средств электронной подписи.

**27 Квалифицированная электронная подпись (далее – КЭП)** – электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи и средств (средства) электронной подписи, получивших (получившего) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом 63-ФЗ;
- ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи.

**28 Сертификат ключа проверки электронной подписи (далее – Сертификат)** – электронный документ или документ на бумажном носителе, выданный Удостоверяющим центром либо Доверенным лицом Удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

По тексту настоящего Регламента употребление термина «Сертификат» означает как Сертификат НЭП, так и Сертификат КЭП.

**29 Средство электронной подписи** – шифровальное (криптографическое) средство, соответствующее следующим признакам:

- используется для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи;
- соответствует требованиям к средствам электронной подписи, утверждённым Приказом ФСБ России от 29.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

**210 Средство удостоверяющего центра** – программное и (или) аппаратное средство, используемое Удостоверяющим центром для выполнения своих функций и соответствующее требованиям к средствам удостоверяющего центра, утверждённым Приказом ФСБ России от 29.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

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

**212 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.

**213 Корпоративная информационная система** – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

**214 Владелец сертификата ключа проверки электронной подписи** (далее Владелец сертификата) – лицо, которому в установленном настоящим Регламентом порядке выдан сертификат ключа проверки электронной подписи, в соответствии с Федеральным законом № 63-ФЗ. Для Сертификата юридического лица вторым Владельцем сертификата является физическое лицо, данные о котором по заявлению юридического лица внесены в его Сертификат (Уполномоченный представитель Заявителя). В случаях, предусмотренных пунктом 3 статьи 14 Федерального закона № 63-ФЗ, данные о физическом лице в Сертификат не вносятся, единственным Владельцем сертификата является юридическое лицо.

**215 Заявитель** – лицо, подающее в Удостоверяющий центр заявление на создание и выдачу квалифицированного сертификата ключа проверки электронной подписи и признающее данный Регламент

**216 Доверенное лицо Заявителя** – физическое лицо, которое действует от имени физического или юридического лица, иного хозяйствующего субъекта, уполномоченное ими на передачу документов для получения Сертификата и получение Сертификата.

**217 Уполномоченный представитель Заявителя (Владельца сертификата)** – физическое лицо, которое действует от имени Заявителя (Владельца сертификата) – юридического лица (индивидуального предпринимателя) или иного хозяйствующего субъекта на основании учредительных документов юридического лица или доверенности и которое указывается в Сертификате данного лица или субъекта в качестве второго Владельца наряду с наименованием первого Владельца сертификата – юридического лица (индивидуального предпринимателя), иного хозяйствующего субъекта.

**218 Уполномоченное лицо Удостоверяющего центра** – работник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по созданию электронных подписей под выдаваемыми Удостоверяющим центром Сертификатами в электронной форме и формируемыми Реестрами отозванных сертификатов, а также иными полномочиями согласно настоящему Регламенту.

**219 Доверенное лицо Удостоверяющего центра** – работник Удостоверяющего центра наделенное Удостоверяющим центром полномочиями по идентификации личности Владельца сертификата, Заявителя или Доверенного лица Заявителя, вручению ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром при наличии лицензии на данную деятельность, а также иными полномочиями согласно настоящего Регламента.

**220 Пользователь** - юридическое лицо, индивидуальный предприниматель или физическое лицо, заключившее договор с Удостоверяющим центром и признающее данный Регламент. Пользователь может не являться владельцем квалифицированного сертификата (Заявителем).

**221 Реестр сертификатов** – реестр выданных и отозванных Удостоверяющим центром Сертификатов, включающий в себя информацию, содержащуюся в выданных этим Удостоверяющим центром Сертификатах, информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях такого прекращения и аннулирования.

**222 Профиль Сертификата** – документ, определяющий области применения, структуру и содержимое полей Сертификатов, а также и перечень документов, необходимых для создания таких Сертификатов.

### **3. Общие положения**

#### **3.1 Статус Регламента**

3.1.1 Регламент оказания услуг Удостоверяющего центра (далее – Регламент) – документ, определяющий условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Удостоверяющего центра, Заявителя и Владельца сертификата, форматы данных, организационные мероприятия, направленные на обеспечение работы Удостоверяющего центра.

3.1.2 Любое заинтересованное лицо может ознакомиться с Регламентом на сайте Удостоверяющего центра по адресу [http://xn----7sblqm4b.xn--p1ai/?page\\_id=23](http://xn----7sblqm4b.xn--p1ai/?page_id=23)

#### **3.2 Субъекты, на которых распространяет свое действие настоящий Регламент**

3.2.1 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.

#### **3.3 Порядок присоединения к Регламенту**

3.3.1 Лицо, заключившее с Удостоверяющим центром договор на оказание услуг Удостоверяющего центра по выдаче 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.

3.3.2 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 (по форме Приложения № 3 к настоящему Регламенту).

#### **3.4 Изменения (дополнения) Регламента**

3.4.1 Внесение изменений (дополнений) в Регламент, в том числе в Приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

3.4.2 Уведомление Субъектов о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем публикации на сайте по адресу [http://xn----7sblqm4b.xn--p1ai/?page\\_id=23](http://xn----7sblqm4b.xn--p1ai/?page_id=23).

3.4.3 Изменения (дополнения), вносимые Удостоверяющим центром в Регламент, кроме изменений (дополнений), вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон по истечению 10 (Десяти) календарных дней с даты их публикации на сайте по адресу [http://xn----7sblqm4b.xn--p1ai/?page\\_id=23](http://xn----7sblqm4b.xn--p1ai/?page_id=23)

3.4.4 Изменения (дополнения), вносимые Удостоверяющим центром в Регламент в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих нормативных актов.

3.4.5 Неотъемлемой частью настоящего Регламента являются Профили сертификатов. Удостоверяющий центр вносит изменения в Профили сертификатов путем публикации их обновленных версий по адресу [http://xn----7sblqm4b.xn--p1ai/?page\\_id=23](http://xn----7sblqm4b.xn--p1ai/?page_id=23). Изменения в Профили сертификатов вступают в силу в порядке пункта 3.4.3 Регламента.

#### **3.5 Перечень услуг, предоставляемых Удостоверяющим центром**

3.5.1 Создание Сертификатов в электронной форме.

3.5.2 Изготовление заверенных копий Сертификатов на бумажном носителе по запросу.

3.5.3 Выдача Правил обеспечения безопасности использования электронной подписи и средств электронной подписи, содержащих условия и порядок использования сертификатов

ЭП, ключей ЭП и средств ЭП.

354 Создание Ключей проверки и Ключей электронной подписи с гарантией обеспечения конфиденциальности Ключей электронной подписи.

355 Предоставление возможности Заявителю создать Ключи проверки и Ключи электронной подписи с гарантией обеспечения конфиденциальности Ключей электронной подписи в Удостоверяющем центре, имеющих необходимые лицензии.

356 Выдача Средств электронной подписи, обеспечивающих возможность создания Ключа электронной подписи и Ключа проверки.

357 Представление по запросу Участников электронного взаимодействия Сертификатов, внесённых в Реестр выданных сертификатов Удостоверяющего центра, в форме электронных документов.

358 Прекращение действия Сертификатов по запросам Владельцев сертификатов и в иных случаях, установленных Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и Заявителем, а также настоящим Регламентом. Услуга оказывается путём внесения сведений о прекращении действия в Реестр отозванных сертификатов.

359 Предоставление сведений об аннулированных Сертификатах и Сертификатах, действие которых прекращено, в том числе опубликование Реестра отозванных сертификатов по адресам, вносимым в соответствующее дополнение Сертификатов.

35.10 Проверка действительности ЭП, Ключи проверки которых содержатся в Сертификатах, выданных Удостоверяющим центром, в Электронных документах.

### **3.6 Информирование Субъектов**

3.6.1 Информирование Субъектов Удостоверяющим центром производится посредством направления электронного письма на адрес, указанный при обращении и/или ином взаимодействии с Удостоверяющим центром и/или посредством размещения информации на сайте по адресу [http://xn----7sblqm4b.xn--p1ai/?page\\_id=23](http://xn----7sblqm4b.xn--p1ai/?page_id=23).



#### **4. Вознаграждение Удостоверяющего центра**

- 4.1** Удостоверяющий центр осуществляет свою деятельность на платной основе.
- 4.2** Стоимость и состав услуг Удостоверяющего центра определяются прайс-листом, который высылается по запросу с электронной почты uc@diack.ru.
- 4.3** Сроки и порядок расчетов за услуги, оказываемые Удостоверяющим центром, регулируются условиями договоров на оказание услуг Удостоверяющего центра между Удостоверяющим центром и Заявителем.
- 4.4** В случае выполнения внеплановой замены Ключа электронной подписи Удостоверяющего центра Удостоверяющий центр безвозмездно создаёт Сертификаты для всех Владельцев сертификатов, чьи сертификаты прекращают действие в связи с внеплановой заменой.
- 4.5** Удостоверяющий центр в порядке, предусмотренном настоящим Регламентом, безвозмездно предоставляет Сертификаты в форме электронных документов из Реестра выданных сертификатов Удостоверяющего центра, а также безвозмездно публикует Реестр отозванных сертификатов.

## 5. Представление информации и документов

**5.1** Удостоверяющий центр предоставляет Заявителю по его требованию копии документов, на основании которых осуществляет свою деятельность.

**5.2** Удостоверяющий центр выполняет свою обязанность по внесению в Сертификат только достоверной и актуальной информации путем сбора и хранения копий документов и информации, представленных Заявителем.

**5.3** Заявитель представляет в Удостоверяющий центр документы в соответствии с Профилем Сертификата (Приложение № 7 к настоящему Регламенту).

**5.4** Если для подтверждения каких-либо сведений, вносимых в Сертификат, действующим законодательством или настоящим Регламентом установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

**5.5** При обращении в Удостоверяющий центр Доверенного лица или Уполномоченного представителя Заявителя его полномочия должны быть подтверждены соответствующей доверенностью/ приказом или иным документом.

**5.6** Надлежащим способом заверения копий документов может являться нотариальное заверение копий, заверение копий органом власти (например, налоговыми органами), заверение копий документов Заявителем самостоятельно.

**5.7** Нотариально заверенные копии документов должны содержать штамп нотариуса «копия верна», штамп с информацией о нотариусе, должны быть заверены печатью нотариуса и иметь подпись нотариуса.

**5.8** Копии, заверенные Заявителем, могут предоставлять исключительно юридические лица и индивидуальные предприниматели. Многостраничные копии либо должны быть прошиты и заверены на листе сшивки, либо на каждой странице такой копии должна иметься отдельная заверительная надпись. Образец заверительной надписи:

ВЕРНО

Должность с указанием наименования организации/индивидуального предпринимателя

Подпись Расшифровка подписи (фамилия и инициалы)

Дата заверения документа

Оттиск печати

**5.9** Копии документов, заверенные органом власти, должны содержать подпись и расшифровку подписи должностного лица, их заверившего, а также печать/штамп данного органа власти.

**5.10** К документам, оформленным на языке, отличном от русского, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

**5.11** 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.

**5.12** Если Заявитель выступает в интересах третьих лиц, то, по требованию Удостоверяющего центра, представляет документы, подтверждающие такие полномочия.

## **6. Права и обязанности Субъектов**

### **6.1 Права Участников электронного взаимодействия**

- 6.1.1 Использовать Реестр отозванных сертификатов для проверки действительности Сертификатов, созданных и выданных Удостоверяющим центром.
- 6.1.2 Получить Сертификат Удостоверяющего центра.
- 6.1.3 Получить информацию, содержащуюся в Реестре выданных сертификатов Удостоверяющего центра.
- 6.1.4 Применять Сертификат для проверки ЭП в электронных документах.
- 6.1.5 Обратиться в Удостоверяющий центр за проверкой подлинности ЭП, созданной с помощью Сертификата, выданного Удостоверяющим центром.
- 6.1.6 При обращении за выдачей Сертификата получить информацию о рисках, связанных с использованием ЭП.

### **6.2 Обязанности Участников электронного взаимодействия**

- 6.2.1 Обеспечивать конфиденциальность Ключей ЭП, в частности, не допускать использование принадлежащих им Ключей ЭП без их согласия.
- 6.2.2 Использовать ЭП в соответствии с ограничениями, содержащимися в Сертификате ключа проверки этой электронной подписи.
- 6.2.3 Уведомлять Удостоверяющий центр, выдавший Сертификат, и иных Участников электронного взаимодействия о нарушении конфиденциальности Ключа электронной подписи в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении.
- 6.2.4 Не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
- 6.2.5 Использовать для создания и проверки ЭП, ключа проверки ЭП и ключа ЭП средства электронной подписи в соответствии с Федеральным законом № 63-ФЗ.

### **6.3 Права Владельца сертификата**

- 6.3.1 Обратиться в Удостоверяющий центр для прекращения действия выданного ему Сертификата в течение срока его действия.
- 6.3.2 Получить средства (средство) электронной подписи, получившие (получившее) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ.
- 6.3.3 Получить под расписку от Удостоверяющего центра Правила обеспечения безопасности использования электронной подписи и средств электронной подписи.

### **6.4 Обязанности Владельца сертификата**

- 6.4.1 Все обязанности, предусмотренные пунктом 6.2. настоящего Регламента.
- 6.4.2 Обеспечить выполнение Правил по обеспечению безопасности на рабочем месте (Приложение № 8).
- 6.4.3 Обеспечивать конфиденциальность Ключей электронных подписей, в частности, не допускать использование принадлежащих им Ключей электронных подписей без их согласия.
- 6.4.4 Не использовать Ключ электронной подписи, Сертификат ключа проверки которой выдан Удостоверяющим центром, и немедленно обратиться в Удостоверяющий центр для прекращения действия этого Сертификата, при наличии оснований полагать, что конфиденциальность этого Ключа электронной подписи нарушена.

6.4.5 Уведомлять Удостоверяющий центр о нарушении конфиденциальности Ключа электронной подписи, Сертификат которой выдан Удостоверяющим центром, в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении.

6.4.6 При выдаче Сертификата ознакомиться с информацией, включаемой в Сертификат, подтвердив этот факт предоставлением расписки в соответствии с пунктом 8.2.4 Регламента.

6.4.7 В случае самостоятельного создания Ключа электронной подписи предоставить Удостоверяющему центру запрос на сертификат в формате, описанном в рекомендациях IETF RFC 2986 “PKCS #10: Certification Request Syntax Specification (2000)” и IETF RFC 4491 “Using GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Inter-net X.509 Public Key Infrastructure Certificate and CRL Profile”, с выполнением требований, предъявляемых к таким электронным документам используемыми Удостоверяющим центром Средствами удостоверяющего центра. Запрос на Сертификат должен содержать всю информацию, представляемую для включения в выдаваемый Сертификат, сведения о Средствах электронной подписи, использовавшихся для создания Ключа электронной подписи и Ключа проверки, и о Средствах электронной подписи, с которыми будет использоваться Сертификат.

### **6.5 Права Удостоверяющего центра**

6.5.1 Запросить у Заявителя документы для подтверждения любой содержащейся в заявлении на выдачу Сертификата информации, а также документы, необходимые для разрешения противоречий между данными в заявлении на выдачу Сертификата и данными в иных представленных документах.

6.5.2 Не принимать документы, не соответствующие требованиям действующих нормативных актов Российской Федерации, информационных систем, на которых планируется использовать Сертификат, требованиям настоящего Регламента и Профиля Сертификата.

6.5.3 Отказать в выдаче Сертификата в случае невыполнения обязанностей, указанных в разделе 6.7 Регламента, а также в случае, если услуга по созданию и выдаче Сертификата не оплачена в надлежащем порядке.

6.5.4 Отказать в выдаче Сертификата в случае подачи Заявления изготовление Сертификата в неактуальной форме, с ошибками, исправлениями, подчистками и/или приписками, не подтвержденными собственноручной подписью Уполномоченного представителя Заявителя или Заявителя-физического лица.

6.5.5 Отказать в выдаче Сертификата в случае, если Заявитель-физическое лицо или Уполномоченный представитель Заявителя не предоставил письменного согласия на обработку своих персональных данных.

6.5.6 Отказать в выдаче Сертификата в случае, если не было подтверждено, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения Сертификата.

6.5.7 Отказать в прекращении действия Сертификата в случае ненадлежащего оформления заявления на прекращение действия Сертификата, а также в случае, если Сертификат аннулирован или прекратил своё действие по другим основаниям.

6.5.8 Без уведомления прекратить действие Сертификата в случае невыполнения Владелец сертификата обязанностей, указанных в разделе 6.4 Регламента, а также в случае появления достоверных сведений о том, что документы, представленные в соответствии с разделом 6.7 настоящего Регламента, не являются подлинными или не подтверждают достоверность всей информации, включённой в данный Сертификат, и/или в случае нарушения Владелец сертификата условий договора, заключенного с Удостоверяющим центром.

6.5.9 Прекратить действие Сертификата в случае получения Удостоверяющим центром подтверждения факта смерти Владельца сертификата-физического лица, факта внесения в Единый государственный реестр юридических лиц записи о ликвидации Владельца сертификата-юридического лица, факта утраты силы государственной регистрации Владельца сертификата-физического лица в качестве индивидуального предпринимателя, главы крестьянского (фермерского) хозяйства, а также в случае вступления в силу судебного решения о дисквалификации Уполномоченного представителя Владельца сертификата.

6.5.10 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.

6.5.11 Использовать представленные Заявителем номера мобильной связи и адреса электронной почты для рассылки уведомлений об окончании срока действия Сертификата, аутентификационной информации в соответствии с пунктом 8.2.5 настоящего Регламента и иной информации.

6.5.12. Прекратить действие Сертификата при наличии у Удостоверяющего центра оснований полагать, что конфиденциальность закрытого ключа электронной подписи нарушена.

## **6.6 Обязанности Удостоверяющего центра**

6.6.1 Использовать для создания Сертификатов Средства Удостоверяющего центра, получившие подтверждение соответствия требованиям действующего законодательства.

6.6.2 Оказывать услуги в соответствии с требованиями, устанавливаемыми Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами.

6.6.3 Вносить в создаваемые Сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами.

6.6.4 Обеспечивать круглосуточную доступность Реестра отозванных сертификатов в сети Интернет, за исключением периодов планового или внепланового технического обслуживания.

6.6.5 Обеспечивать актуальность информации, содержащейся в Реестре выданных сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

6.6.6 В случае принятия решения о прекращении своей деятельности без передачи функции Удостоверяющего центра другим лицам сообщить об этом на сайте [http://xn----7sblqm4b.xn--p1ai/?page\\_id=23](http://xn----7sblqm4b.xn--p1ai/?page_id=23) и в уполномоченный федеральный орган не позднее, чем за 1 (Один) месяц до даты прекращения своей деятельности, и передать в уполномоченный федеральный орган Реестр выданных сертификатов.

6.6.7 Внести сведения о выданном Сертификате в Реестр выданных сертификатов.

6.6.8 Произвести регистрацию квалифицированного сертификата ЭП в Единой системе идентификации и аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона № 63-ФЗ.

6.6.9 Исполнять прочие обязанности, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и иными нормативными актами.

## **6.7 Обязанности Заявителя**

6.7.1 Предъявить документы, удостоверяющие личность Доверенного лица Заявителя, Уполномоченного представителя Заявителя, Заявителя-физического лица в соответствии с разделом 5 настоящего Регламента.

6.7.2 Обеспечить личную явку в Удостоверяющий центр Заявителя либо его представителя

6.7.3 Представить в Удостоверяющий центр документы, предусмотренные Федеральным законом № 63-ФЗ, другими Федеральными законами и принимаемыми в соответствии с ними нормативными актами, локальными документами отдельных информационных систем, и иные необходимые для создания Сертификата документы. Перечень документов, необходимых для создания Сертификата, определяется Профилем Сертификата с учетом положений пункта 6.5.1 настоящего Регламента.

6.7.4 В случае изменения данных, содержащихся в документах согласно Профиля Сертификата, с момента предоставления указанных документов до момента выдачи Сертификата, сообщать Удостоверяющему центру о таких изменениях. Ответственность за правильность и актуальность данных в предоставленных документах и данных на момент выпуска Сертификата несет Заявитель.

6.7.5 По требованию Удостоверяющего центра обеспечить личную явку определенных представителей Заявителя, а также совершить иные действия, направленные на обеспечение безопасности и законности процесса выдачи Сертификата (в том числе с использованием различных технических средств).

## **7. Ответственность субъектов**

**7.1** Удостоверяющий центр в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

7.1.1 неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг Удостоверяющего центра;

7.1.2 неисполнения или ненадлежащего исполнения обязанностей, предусмотренных действующим законодательством и настоящим Регламентом.

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

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

- 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.

**7.4** 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. Удостоверяющий центр не несет ответственность за действия владельцев информационных систем, приведших к невозможности использования Сертификатов ключей подписи в этих информационных системах.

## **8. Порядок оказания услуг Удостоверяющего центра**

### **8.1 Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим Центром**

Заявитель вправе создать ключ электронной подписи и ключ проверки электронной подписи самостоятельно с использованием следующих способов:

1. На рабочем месте Заявителя, с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи» и совместимого со средствами и электронной подписи, используемыми в Удостоверяющем центре по форматам ключей и Сертификатов;

При реализации данного способа Заявитель обеспечивает конфиденциальность ключа электронной подписи с момента его создания. При обращении в Удостоверяющий центр предоставить файл запроса в формате PKCS # 10, содержащий ключ проверки электронной подписи и информацию идентифицирующую владельца ключа проверки электронной подписи в объеме, определенном Федеральным законом «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

При обращении в Удостоверяющий центр с заявлением на изготовление и выдачу квалифицированного сертификата Заявитель должен подтвердить владение ключом электронной подписи. Подтверждение владения ключом электронной подписи производится путем проверки электронной подписи в файле запроса на квалифицированный Сертификат, который предоставляет заявитель, с использованием средств удостоверяющего центра. При отрицательном результате проверки электронной подписи в предоставленном файле запроса на квалифицированный Сертификат удостоверяющий центр отказывает заявителю в изготовлении и выдаче квалифицированного Сертификата.

2. С использованием автоматизированного рабочего места Удостоверяющего центра при обращении с заявлением на создание и выдачу квалифицированного Сертификата. Создание ключей электронной подписи осуществляется Заявителем самостоятельно или выполняется сотрудником удостоверяющего центра в присутствии Заявителя.

При реализации данного способа используется автоматизированное рабочее место, аттестованное на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации, размещенное в аттестованном помещении, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается на ключевой носитель, предназначенный для хранения ключевой информации и сертифицированный в установленном порядке по требованиям защиты информации, который выдается заявителю либо доверенному лицу заявителя по окончании процедуры выдачи Сертификата.

### **8.2. Порядок подключения (регистрации) пользователей**

8.2.1. Пользователь заключает договор с Удостоверяющим центром и производит оплату.

8.2.2. Пользователь представляет Удостоверяющему центру заявление на изготовление квалифицированного Сертификата ключа проверки электронной подписи, содержащее:

- данные на сотрудников, которым необходимо создать ключи ЭП и/или изготовить Сертификат;

8.2.3. Уполномоченное лицо Удостоверяющего центра согласует с Пользователем



график выполнения работ.

8.2.4. В соответствии с согласованным графиком работ, владельцы Сертификата (заявители), указанные в заявлении Пользователя, лично или их доверенные лица, прибывают в офис Удостоверяющего центра, где:

- получают СКЗИ и ключи и/или Сертификат;
- подписывают акт о получении СКЗИ, ключей ЭП, Сертификата;
- расписываются в Сертификате на бумажном носителе, подтверждая достоверность информации, внесенной в Сертификат;
- получают в электронном виде актуальный Сертификат Удостоверяющего центра;
- получают пароль для связи на случай компрометации ключей;
- получают инструктаж и руководство (памятку) об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

Примечание: допускается вместо бумажных документов оформление электронных документов с ЭП уполномоченных лиц, если это не запрещено ФЗ или нормативно-правовыми актами.

### **8.3. Порядок подачи заявления на создание и выдачу квалифицированного Сертификата**

8.3.1. Актуальная форма заявления на изготовление и выдачу квалифицированного Сертификата ключа проверки электронной подписи публикуется на официальном сайте Удостоверяющего центра <http://диас-к.рф> (Приложение № 4 к Регламенту)

8.3.2. Заявитель или его законный представитель вправе обратиться в офис Удостоверяющего центра, с заявлением и документами, необходимыми для выпуска квалифицированного Сертификата.

### **8.4. Требования к оформлению заявления на создание и выдачу квалифицированного Сертификата**

8.4.1. При оформлении заявления на создание и выдачу квалифицированного Сертификата на физическое лицо в заявлении указывается:

- фамилия, имя и отчество заявителя полностью, без сокращений;
  - индивидуальный номер налогоплательщика (ИНН) физического лица;
  - сведения о документе, удостоверяющем личность заявителя (вид документа, серия, номер, кем выдан документ и дата его выдачи);
  - страховой номер индивидуального лицевого счета (СНИЛС);
  - адрес электронной почты и телефон для связи с заявителем;
  - адрес регистрации по месту жительства (пребывания);
- назначение использования квалифицированного Сертификата (при необходимости).

8.4.2. При оформлении заявления на создание и выдачу квалифицированного Сертификата на физическое лицо - представителя юридического лица в заявлении указываются:

- полное или сокращенное наименование юридического лица в соответствии с уставными документами;
- должность, фамилия, имя отчество руководителя юридического лица;
- индивидуальный номер налогоплательщика (ИНН) юридического лица, код причины постановки на учет в налоговом органе и основной государственный регистрационный номер юридического лица;
- фамилия, имя, отчество заявителя полностью;

- сведения о документе, удостоверяющем личность заявителя (вид документа, серия, номер, кем выдан документ и дата его выдачи);
- страховой номер индивидуального лицевого счета (СНИЛС) физического лица - заявителя;
- адрес электронной почты и телефон для связи с заявителем;
- адрес места нахождения юридического лица в соответствии с регистрационными документами;
- назначение использования квалифицированного Сертификата (при необходимости).

8.4.3. В заявлении указывается, что заявитель ознакомлен с настоящим Регламентом и обязуется его выполнять, выражает свое согласие на обработку, передачу и хранение предоставленных персональных данных в целях изготовления и обслуживания Сертификата и гарантирует достоверность и подлинность предоставленных данных, признает, что персональные данные, заносимые в квалифицированный Сертификат, относятся к общедоступным персональным данным. Указанные сведения подтверждаются личной подписью заявителя с указанием даты заполнения заявления.

В случае подачи заявления представителем юридического лица достоверность данных дополнительно подтверждается подписью руководителя и печатью организации.

8.4.4. Заявление может быть предоставлено в удостоверяющий центр как на бумажном носителе, так и в электронной форме. В случае подачи Заявления в электронной форме, оно должно быть подписано квалифицированной электронной подписью заявителя и может быть направлено с использованием сети Интернет. При последнем способе подачи Пользователь самостоятельно несет ответственность за сохранение конфиденциальности персональных данных, содержащихся в заявлении.

8.4.5. Вместе с заявлением на создание и выдачу квалифицированного Сертификата Пользователь предоставляет в Удостоверяющий центр перечень документов, определенный Разделом 8.6 настоящего Регламента.

## **8.5. Порядок установления личности заявителя**

8.5.1. В случае личного обращения заявителя в Удостоверяющий центр для подачи заявления и/или получения квалифицированного Сертификата сотрудники Удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» обязаны установить личность заявителя или его представителя:

- личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность, - паспорту гражданина Российской Федерации.
- личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства, с учетом требований Раздела 8.6 настоящего Регламента;
- личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц;

## **8.6. Перечень документов, запрашиваемых Удостоверяющим Центром у Заявителя для изготовления и выдачи Сертификата, в том числе для удостоверения личности заявителя, а также требования к таким документам**

При обращении в удостоверяющий центр заявитель или его доверенное лицо предоставляет документы необходимые для установления личности заявителя (его доверенного лица), а также документы (или их надлежащим образом заверенные копии), подтверждающие сведения, на основании которых удостоверяющим центром вносятся

данные в квалифицированный Сертификат.

8.6.1. В случае изготовления квалифицированного Сертификата на Заявителя - физическое лицо, в удостоверяющий центр предоставляются следующие документы (оригиналы или их надлежащим образом заверенные копии):

- основной документ, удостоверяющий личность заявителя (его доверенного лица) в соответствии с требованиями Раздела 8.5 настоящего Регламента;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- нотариальная доверенность (в случае если от имени заявителя действует доверенное лицо).

• В случае изготовления квалифицированного Сертификата на физическое лицо - представителя юридического лица, в удостоверяющий центр представляются следующие документы:

- основной документ, удостоверяющий личность в соответствии с требованиями Раздела 8.5 настоящего Регламента;
- номер страхового свидетельства государственного пенсионного страхования
- копия свидетельства о государственной регистрации юридического лица, заверенная руководителем юридического лица и печатью юридического лица
- копия свидетельства о постановке на учет в налоговом органе, заверенная руководителем юридического лица и печатью юридического лица
- копия решения (протокола) о назначении или об избрании руководителя или доверенность на право обращения за получением квалифицированного Сертификата, заверенные подписью руководителя и печатью юридического лица.

8.6.2. В случае изготовления квалифицированного Сертификата на лицо, выступающее от имени заявителя - иностранной организации предоставляет в удостоверяющий центр следующие документы:

- основной документ, удостоверяющий личность в соответствии с требованиями Раздела 8.5 настоящего Регламента;
- номер свидетельства о постановке на учет в налоговом органе или идентификационный номер налогоплательщика заявителя - иностранной организации;
- доверенность или иной документ, подтверждающий полномочия обращаться за получением квалифицированного Сертификата.

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

Если для подтверждения каких-либо сведений, вносимых в Сертификат, действующим законодательством установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

Удостоверяющий центр вправе потребовать у заявителя дополнительные документы для подтверждения сведений, включаемых в квалифицированный Сертификат.

## **8.7. Порядок создания и выдачи квалифицированного Сертификата**

8.7.1. Удостоверяющий центр с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем для изготовления и выдачи Сертификата, в том числе запрашивает и получает из государственных информационных ресурсов:

- выписку из единого государственного реестра юридических лиц - в отношении заявителя - юридического лица;

- выписку из единого государственного реестра индивидуальных предпринимателей - в отношении заявителя - индивидуального предпринимателя;
- выписку из Единого государственного реестра налогоплательщиков - в отношении заявителя - иностранной организации.

8.7.2. В случае, если полученные из государственных реестров сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный Сертификат, и удостоверяющим центром установлена личность заявителя - физического лица или получено подтверждение полномочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного Сертификата, удостоверяющий центр создает ключи электронной подписи (при необходимости) и квалифицированный Сертификат.

8.7.3. Если представленные заявителем данные не подтверждены, удостоверяющий центр отказывает в создании квалифицированного Сертификата.

8.7.4. Удостоверяющий центр выдает квалифицированный Сертификат заявителю в электронной форме. При выдаче квалифицированного Сертификата заявителю для ознакомления с информацией, содержащейся в квалифицированном Сертификате, предоставляется копия квалифицированного Сертификата на бумажном носителе в двух экземплярах.

8.7.5 Заявитель подтверждает корректность данных, внесенных в квалифицированный Сертификат, собственноручной подписью на бумажных экземплярах Сертификата, один из которых остается у заявителя, второй экземпляр - передается на архивное хранение в Удостоверяющий центр.

8.7.6. Вместе с квалифицированным Сертификатом заявителю передается парольная группа, используемая для аутентификации Пользователя Удостоверяющего центра при выполнении регламентных процедур, возникающих при нарушении конфиденциальности ключевых документов Пользователя.

8.7.7. Заявитель информируется в письменной форме об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

8.7.8. Срок создания и выдачи квалифицированного Сертификата не превышает 5 (пяти) рабочих дней с момента подачи заявления и комплекта подтверждающих документов, при условии оплаты услуг по созданию и выдаче квалифицированного сертификата.

## **8.8. Прекращение действия и аннулирование Сертификата**

8.8.1. Сертификат прекращает свое действие:

- по истечении срока его действия;
- по заявлению Владельца сертификата о прекращении действия Сертификата. Форма такого заявления приведена в Приложении № 3 к настоящему Регламенту. Также заявление о прекращении действия ранее выданного Сертификата может содержаться в составе Заявления на выдачу Сертификата;
- по решению Удостоверяющего центра в случаях, предусмотренных пунктами 6.5.8 настоящего Регламента;
- в случае прекращения деятельности Удостоверяющего центра без передачи его функций другим лицам.

8.8.2. Удостоверяющий центр признает Сертификат аннулированным, если:

- не подтверждено, что Владелец сертификата владеет Ключом ЭП, соответствующим Ключу проверки ЭП, указанному в таком Сертификате;

- установлено, что содержащийся в Сертификате Ключ проверки ЭП уже содержится в ином ранее созданном Сертификате;
- вступило в силу решение суда, которым установлено, что Сертификат содержит недостоверную информацию.

8.8.3. Доверенное лицо Удостоверяющего центра при приеме заявления на прекращение действия Сертификата получает от лица, выступающего от имени Владельца сертификата, подтверждение правомочия обращаться за прекращением действия Сертификата. Приём заявлений осуществляется в Удостоверяющем центре в рабочие дни в рабочее время (не ранее 9:00 и не позднее 18:00 местного времени).

8.8.4. Информация о прекращении действия или аннулировании Сертификата вносится в Реестр отозванных сертификатов. Действие Сертификата прекращается с момента публикации в Реестре отозванных сертификатов, в который внесён этот Сертификат. Срок внесения в Реестр отозванных сертификатов сведений о прекращении действия или аннулировании Сертификата составляет не более 72 (семидесяти двух) часов с момента приема заявления на прекращение действия Сертификата или наступления иного события, предусмотренного пунктами 8.8.1, 8.8.2 настоящего Регламента. Более короткий срок может устанавливаться в Профиле сертификата.

### **8.9. Прекращение действия Сертификата**

8.9.1 Удостоверяющий центр вправе по собственной инициативе приостановить действие выданного им Сертификата для проверки поступившей информации об обстоятельствах, влекущих прекращение действия или аннулирование Сертификата по причинам, предусмотренным пунктами 6.5.8, 6.5.9, 6.5.12, 8.8.2 настоящего Регламента.

8.9.2. О прекращении действия Сертификата Удостоверяющий центр уведомляет Владельца сертификата по адресу электронной почты, указанному в прекращенном Сертификате.

8.9.3. Стоимость Сертификата за период времени, когда его действие было прекращено, Владельцу сертификата не возвращается и иным образом не компенсируется.

### **8.10 Порядок предоставления доступа к Реестру выданных сертификатов**

8.10.1. Доступ к Реестру выданных сертификатов осуществляется безвозмездно на основании запроса в свободной форме с указанием информации, позволяющей идентифицировать Сертификат в Реестре выданных сертификатов, и цели, для достижения которой должен быть представлен доступ к Реестру. Сведения из Реестра выданных сертификатов по каждому отдельному выданному Сертификату представляются на основании отдельного запроса.

8.10.2 Доступ к Реестру выданных сертификатов предоставляется путем представления Сертификата в форме электронного документа, либо в форме копии Сертификата на бумажном носителе.

8.10.3 Срок представления Удостоверяющим центром сведений из Реестра выданных сертификатов составляет 7 (семь) рабочих дней с момента получения Удостоверяющим центром запроса на предоставление информации.

### **8.11 Подтверждение подлинности ЭП Удостоверяющего центра в выданных Сертификатах**

8.11.1. Подтверждение подлинности ЭП Удостоверяющего центра осуществляется на основании заявления, форма которого установлена Приложением № 1 к настоящему Регламенту.

8.11.2 Срок проведения экспертизы составляет 15 (Пятнадцать) рабочих дней с момента поступления заявления в Удостоверяющий центр при условии поступления оплаты стоимости данной услуги на расчетный счет Удостоверяющего центра.

## **8.12 Подтверждение подлинности ЭП в электронных документах**

8.12.1. Подтверждение подлинности ЭП в электронном документе, авторство или содержание которого оспаривается, осуществляется на основании заявления на подтверждение подлинности ЭП, форма которого установлена Приложением № 2 к настоящему Регламенту.

8.12.2 К заявлению прикладывается электронный документ и ЭП, подтверждение которой производится.

8.12.3 Проверка ЭП под электронными документами, созданными не Удостоверяющим центром, при технической совместимости используемых средств УЦ производится при представлении правил документирования, в соответствии с которыми были созданы электронный документ и проверяемая ЭП.

8.12.4 Срок проведения работ по подтверждению подлинности ЭП в электронном документе составляет 15 (пятнадцать) рабочих дней с момента поступления заявления в Удостоверяющий центр и при условии поступления оплаты стоимости данной услуги на расчетный счет Удостоверяющего центра.

8.12.5 При проведении работ Удостоверяющим центром может быть запрошена дополнительная информация.

## **9. Прочие условия**

### **9.1 Конфиденциальность**

9.1.1 Удостоверяющий центр обеспечивает конфиденциальность персональных данных, вносимых в Реестр сертификатов.

### **9.2 Плановая замена Ключей Удостоверяющего центра**

9.2.1 Плановая замена Ключей Удостоверяющего центра (Ключа ЭП и соответствующего ему Ключа проверки ЭП) выполняется не ранее, чем через 1 (Один) год и не позднее, чем через 1 (Один) год и 3 (Три) месяца после начала действия соответствующего Ключа.

9.2.2 Процедура плановой замены Ключей осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего центра формирует новый Ключ электронной подписи и соответствующий ему Ключ проверки электронной подписи;
- Уполномоченное лицо Удостоверяющего центра изготавливает Сертификат и подписывает его созданным Ключом электронной подписи.

9.2.3 Старый Ключ электронной подписи (подвергшийся процедуре плановой замены) Удостоверяющего центра используется в течение своего срока действия для формирования Реестра отозванных сертификатов из числа тех Сертификатов, которые были созданы в период действия старого Ключа электронной подписи.

### **9.3 Внеплановая замена Ключей Удостоверяющего центра**

9.3.1 В случае компрометации или угрозы компрометации Ключа электронной подписи Удостоверяющего центра выполняется внеплановая замена соответствующего Ключа.

9.3.2 Процедура внеплановой замены Ключей Удостоверяющего центра выполняется в порядке, определенном процедурой плановой замены таких Ключей, согласно разделу 9.2 настоящего Регламента.

9.3.3 Одновременно прекращается действие всех Сертификатов, подписанных этим Ключом электронной подписи, с занесением сведений об этих сертификатах в Реестр отозванных сертификатов.

9.3.4 После выполнения процедуры внеплановой замены Ключа электронной подписи Удостоверяющего центра прекращается действие Сертификата Ключа проверки электронной подписи, Ключ электронной подписи которого подвергнут процедуре внеплановой замены.

9.3.5 Реестр отозванных сертификатов подписывается старым Ключом электронной подписи (подвергшимся процедуре внеплановой замены).

9.3.6 Удостоверяющий центр информирует Владельцев сертификатов, которые прекращают свое действие, о факте внеплановой замены Ключей Удостоверяющего центра.

9.3.7 После получения официального уведомления о факте внеплановой замены Ключей Удостоверяющего центра Владельцам сертификатов необходимо выполнить процедуру создания и выдачи новых Сертификатов в соответствии с порядком, установленным пунктами 8.1 – 8.2 настоящего Регламента.

### **9.4 Нарушение конфиденциальности Ключа электронной подписи Владельца сертификата**

9.4.1 В случае нарушения конфиденциальности Ключа электронной подписи, а также в случаях наличия оснований полагать, что конфиденциальность Ключа электронной подписи была нарушена, Владелец сертификата Ключа проверки электронной подписи, соответствующего такому Ключу электронной подписи, должен прекратить использование этого Ключа и подать в Удостоверяющий центр заявление на прекращение

действия этого Сертификата.

### **9.5 Сроки действия Ключей и Сертификатов**

9.5.1 Срок действия Ключей электронной подписи Удостоверяющего центра составляет не более 3 (трех) лет. Начало периода действия Ключей электронной подписи Удостоверяющего центра исчисляется с момента начала действия его Сертификата.

9.5.2 Срок действия Сертификата Удостоверяющего центра составляет не более 15 лет.

9.5.3 Срок действия Ключа электронной подписи Владельца Сертификата составляет не более 15 (пятнадцати) месяцев. Начало периода действия Ключа электронной подписи Владельца сертификата исчисляется с момента начала действия Сертификата.

9.5.4 Срок действия Сертификата, соответствующего Ключу электронной подписи Владельца сертификата, составляет не более 15 (пятнадцати) месяцев.

### **9.6 Хранение Сертификатов в Удостоверяющем центре**

9.6.1 Хранение в Удостоверяющем центре всех выданных Сертификатов осуществляется постоянно в форме электронных документов.

### **9.7 Структура Сертификатов и Реестра отозванных сертификатов**

9.7.1 Удостоверяющий центр издает Сертификаты в форме электронного документа формата X.509 версии 3 и ведет Реестр отозванных сертификатов в электронной форме формата X.509 версии 2.

9.7.2 Требования к структуре Сертификатов установлены в Профиле Сертификата.



## Приложения

### Приложение № 1 к Регламенту Форма заявления на подтверждение ЭП Удостоверяющего центра в Сертификате

Заявление на подтверждение электронной подписи Удостоверяющего центра  
в Сертификате ключа проверки электронной подписи

место составления

«\_\_» \_\_\_\_\_»20\_\_г.

Прошу подтвердить подлинность электронной подписи Удостоверяющего центра в  
сертификате ключа проверки электронной подписи, серийный номер:

\_\_\_\_\_

выданном на имя \_\_\_\_\_

(указать ФИО Уполномоченного лица Удостоверяющего центра)

и установить статус этого сертификата (действовал/не действовал) на момент

\_\_\_\_\_

(указать дату и время, на момент наступления которых требуется установить подлинность ЭП и статус сертификата)

Приложение: Сертификат ключа проверки электронной подписи в электронном виде.

\_\_\_\_\_

(при необходимости – указать должность  
уполномоченного лица клиента)

\_\_\_\_\_

(подпись)

\_\_\_\_\_

(расшифровка подписи)

М.П.

**Приложение № 2 к Регламенту  
Форма заявления на подтверждение ЭП в электронном документе**

Заявление на подтверждение электронной подписи в электронном документе

место составления

«\_\_»\_\_\_\_\_»20\_\_г.

Прошу подтвердить подлинность электронной подписи в документе:\_\_\_\_\_

\_\_\_\_\_ (указать наименование документа)

со следующими реквизитами:\_\_\_\_\_

(указать имя файла)

Дата подписания документа ЭП: «\_\_»\_\_\_\_\_20\_\_г.

Серийный номер сертификата:\_\_\_\_\_

сертификат выдан на имя:\_\_\_\_\_

(указать ФИО Владельца сертификата)

В ходе проверки также прошу установить статус этого сертификата (действовал/не действовал) на момент подписания документа.

Приложение: электронный документ;

электронная подпись.

\_\_\_\_\_  
(при необходимости – указать должность  
уполномоченного лица клиента)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(расшифровка подписи)

М.П.

**Приложение № 3 к Регламенту  
Форма заявления на прекращение действия Сертификата**

**Заявление  
на прекращение действия Сертификата**

«\_\_» \_\_\_\_\_ 20\_\_ г.

Прошу прекратить действие Сертификата ключа проверки электронной подписи со следующими данными:

Серийный номер	
Организация	
ИНН	
Фамилия Имя Отчество	

В СВЯЗИ С \_\_\_\_\_  
(указать причину: нарушение конфиденциальности ключа подписи, прекращение работы и т. д.)

от имени Владельца сертификата

\_\_\_\_\_  
(должность) (подпись) (расшифровка подписи)

М.П.

по доверенности<sup>1</sup> от «\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Настоящим подтверждаю, что Заявление на прекращение действия Сертификата получено, Серийный номер, Организация, ИНН, Фамилия Имя Отчество, СНИЛС, а также личность и полномочия представителя, подписавшего настоящее Заявление, проверены.

Доверенное лицо  
Удостоверяющего центра

\_\_\_\_\_  
(подпись) (расшифровка подписи)

<sup>1</sup>При подписании настоящего заявления уполномоченным лицом должны быть указаны реквизиты его доверенности.

# Приложение № 4 к Регламенту

## Форма заявления на изготовление квалифицированного сертификата

Заявление на сертификат №		Генеральному директору ООО «ДИАС-К» Р.О. Долинину	
		[ДАТА]	
<b>ЗАЯВЛЕНИЕ</b> <b>на изготовление сертификата ключа проверки электронной подписи</b>			
Я,		[ФИО]	
		[Должность, если применимо]	
		[Организация, если применимо]	
основание полномочий:			
[основание полномочий, если применимо]			
[Вид документа]		[номер документа], выдан	
[Дата выдачи документа]	г.	[место выдачи документа]	
1. Прошу зарегистрировать и сформировать ключ электронной подписи, записать сформированный ключ электронной подписи на ключевой носитель и изготовить квалифицированный сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра ООО «ДИАС-К» в соответствии с данными, указанными в заявлении на выпуск сертификата:			
Наименование		Значение	
Общее имя (2.5.4.3)			
Фамилия (2.5.4.4)			
Имя и отчество (2.5.4.42)			
Страна/регион (2.5.4.6)			
Область/край (2.5.4.8)			
Город (2.5.4.7)			
Адрес (2.5.4.9)			
Организация (2.5.4.10)			
Должность или звание (2.5.4.12)			
СНИЛС (1.2.643.100.3)			
ИНН (1.2.643.3.131.1.1)			
Адрес E-Mail (1.2.840.113549.1.9.1)			
ОГРН (1.2.643.100.1)			
ОГРНИП (1.2.643.100.5)			
Неструктурированное имя (1.2.840.113549.1.9.2)			
Ключевая фраза, используемая для аутентификации пользователя при выполнении регламентных процедур, возникающих при компрометации ключевых документов:			
[ключевая фраза]			
2. В соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра ООО «ДИАС-К», условия которого определены ООО «ДИАС-К» и опубликованы на сайте Удостоверяющего центра ООО «ДИАС-К» по адресу <a href="http://xn----7sblqm4b.xn--p1ai/?page_id=23">http://xn----7sblqm4b.xn--p1ai/?page_id=23</a> С регламентом Удостоверяющего центра по выпуску квалифицированных сертификатов ключа проверки электронной подписи и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа.			
3. Я,		[ФИО]	
[Вид документа]		[номер документа], выдан	
[Дата выдачи документа]	г.	[место выдачи документа]	
В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», даю своё согласие ООО «ДИАС-К» на обработку персональных данных, включаемых в сертификат ключа подписи, в том числе публикацию в общедоступных источниках и сети Интернет по адресам распространения списка отозванных сертификатов и подтверждаю, что обладаю правами доступа, достаточными для чтения и отправки электронных сообщений с помощью ящика электронной почты			
[электронный адрес]			
и даю согласие на использование этого ящика для информационного взаимодействия с ООО «ДИАС-К». Настоящее согласие на обработку персональных данных действует в течение срока действия сертификата ключа подписи и нахождения его в реестре выданных и отозванных сертификатов.			
Подписи:			
Пользователь Удостоверяющего центра			
_____		[ДАТА]	
[ПОДПИСЬ]		[ФИО]	

**Приложение № 5 к Регламенту**  
**Форма доверенности на получение Сертификата**  
**Доверенность №**

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_ (место составления)

Доверитель \_\_\_\_\_

(Для юридических лиц указывается: сокращенное наименование, включая организационно-правовую форму, ИНН, ОГРН, юридический адрес, ФИО, должность уполномоченного лица, документ, устанавливающий основания (устав/приказ/доверенность и т.п.). Для индивидуальных предпринимателей указывается: ИП ФИО, ИНН, ОГРНИП, адрес ИП. Для физических лиц указывается: ФИО, серия и номер паспорта, кем и когда выдан.)

наделяет нижеперечисленными полномочиями следующее лицо (Представителя):

\_\_\_\_\_ (ФИО Представителя)  
паспорт \_\_\_\_\_  
(серия и номер паспорта Представителя, когда выдан)  
выдан \_\_\_\_\_  
(кем выдан)

1. Предоставлять в Удостоверяющий центр ООО «ДИАС-К» необходимые документы, определённые Регламентом оказания услуг Удостоверяющего центра ООО «ДИАС-К», необходимые для изготовления сертификата ключа проверки электронной подписи для Владельца сертификата:

\_\_\_\_\_ (фамилия, имя, отчество лица, на имя которого изготавливается сертификат)

2. Получать сформированные Сертификат(ы) Доверителя, ключи электронных подписей и подписывать расписку в получении Сертификатов.

4. Получать защищённые носители ключевой информации (Рутокен, eToken, JaCarta и т.д.).

5. Получать все необходимые документы, которые предусмотрены Регламентом оказания услуг Удостоверяющего центра ООО «ДИАС-К».

Для осуществления полномочий по настоящей доверенности Представитель наделяется правом подписывать договор на оказание услуг Удостоверяющего центра, дополнительные соглашения к договору, заявления на изготовление Сертификата ключа проверки электронной подписи, первичные бухгалтерские документы, заверять копии документов, представляемых в Удостоверяющий центр, а также собственноручно расписываться во всех необходимых для этого документах.

Настоящая доверенность действительна до « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. без права передоверия.

Подпись Представителя

\_\_\_\_\_ (подпись)

\_\_\_\_\_ (ФИО)

Подпись Доверителя

\_\_\_\_\_ (подпись)

\_\_\_\_\_ (ФИО)

М.П.\*

\* «Место печати» для юридических лиц (при наличии печати) и индивидуальных предпринимателей (при наличии печати).

Удостоверяющий Центр  
Общество с ограниченной ответственностью "ДИАС-К"

Бланк квалифицированного сертификата ключа проверки электронной подписи

Сведения о сертификате:

Версия:

Серийный номер:

Издатель сертификата

Владелец сертификата

Срок действия:

Ключ проверки электронной подписи:

Расширения сертификата X.509

Расширение: Использование ключа (критичное)

Расширение: Улучшенный ключ

Расширение: Средство электронной подписи владельца

Расширение: Идентификатор ключа центра сертификатов

Расширение: Идентификатор ключа субъекта

Расширение: Политики применения

Расширение: Политики сертификата

Расширение: Сведения о шаблоне сертификата

Расширение: Средства электронной подписи и УЦ издателя

Расширение: Точки распространения списков отзыва (CRL)

Расширение: Доступ к информации о центрах сертификации

Подпись Удостоверяющего центра:

С руководством по обеспечению безопасности при использовании квалифицированной электронной подписи ознакомлен(а). Сертификат получил(а).

Подпись владельца сертификата: \_\_\_\_\_ / \_\_\_\_\_  
" \_\_\_\_ " \_\_\_\_\_ 20\_\_ г.

Подпись доверенного лица: \_\_\_\_\_ / \_\_\_\_\_  
" \_\_\_\_ " \_\_\_\_\_ 20\_\_ г.  
М. П.

## Приложение № 7 к Регламенту Профиль квалифицированного сертификата

### Общие сведения о сертификатах

Квалифицированный сертификат выпускается в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ, иными нормативными актами.

Владельцем квалифицированного сертификата может быть юридическое лицо, индивидуальный предприниматель, а также физическое лицо. В случае если владельцем сертификата является юридическое лицо, в сертификат могут быть внесены сведения о физическом лице, уполномоченном представлять юридическое лицо.

В случае изготовления квалифицированного сертификата для автоматического создания и (или) автоматической проверки электронных подписей в отдельных информационных системах при оказании государственных и муниципальных услуг, в такой сертификат не включаются данные о физическом лице.

### Сведения о владельце сертификата

Идентифицирующие данные владельца сертификата содержатся в поле «Subject» в формате X.500 (Distinguished Name).

Атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом, уполномоченным представлять юридическое лицо (уполномоченное лицо), являются:

Наименование	Ограничение длины	Описание
Common Name	64	Наименование организации – обязательно
Surname	40	Фамилия уполномоченного лица – обязательно
Given name	64	Имя и отчество (при наличии) уполномоченного лица – обязательно
Title	64	Наименование должности уполномоченного лица – опционально
Organization	64	Наименование юридического лица – обязательно
Organizational Unit	64	Наименование подразделения, в котором работает уполномоченное лицо, – опционально
Street	128	Часть адреса местонахождения организации, включающая наименование улицы, номер дома, корпуса, строения, квартиры, помещения, – обязательно
Locality	128	Наименование населенного пункта по адресу местонахождения организации – обязательно
State Or Province	128	Код и наименование субъекта РФ по адресу местонахождения организации – обязательно
Country	2	RU
Email	255	Адрес электронной почты уполномоченного лица – обязательно
OGRN	13	ОГРН организации – обязательно
SNILS	11	СНИЛС уполномоченного лица – обязательно
INN	12	ИНН организации – обязательно (первые два разряда заполняются нулями)

Атрибутами поля идентификационных данных Владельца сертификата, являющегося индивидуальным предпринимателем, являются:

Наименование	Ограничение длины	Описание
Common Name	64	Фамилия, имя и отчество (при наличии) индивидуального предпринимателя – обязательно
Surname	40	Фамилия индивидуального предпринимателя – обязательно
Given name	64	Имя и отчество (при наличии) индивидуального предпринимателя – обязательно
Title	64	Наименование должности индивидуального предпринимателя – опционально
Locality	128	Наименование населенного пункта по адресу регистрации индивидуального предпринимателя – обязательно
State Or Province	128	Код и наименование субъекта РФ по адресу регистрации индивидуального предпринимателя – обязательно
Country	2	RU
Email	255	Адрес электронной почты индивидуального предпринимателя – обязательно
OGRNIP	15	ОГРНИП индивидуального предпринимателя – обязательно
SNILS	11	СНИЛС индивидуального предпринимателя – обязательно
INN	12	ИНН индивидуального предпринимателя – обязательно

Атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом и уполномоченным представлять индивидуального предпринимателя (уполномоченное лицо), являются:

Наименование	Ограничение длины	Описание
Common Name	64	Фамилия, имя и отчество (при наличии) индивидуального предпринимателя – обязательно
Surname	40	Фамилия уполномоченного лица – обязательно
Given name	64	Имя и отчество (при наличии) уполномоченного лица – обязательно
Title	64	Наименование должности уполномоченного лица – опционально
Locality	128	Наименование населенного пункта по адресу регистрации индивидуального предпринимателя – обязательно
State Or Province	128	Код и наименование субъекта РФ по адресу регистрации индивидуального предпринимателя – обязательно
Country	2	RU



Email	255	Адрес электронной почты уполномоченного лица – обязательно
OGRNIP	15	ОГРНИП индивидуального предпринимателя – обязательно
SNILS	11	СНИЛС уполномоченного лица – обязательно
INN	12	ИНН индивидуального предпринимателя – обязательно

Сертификаты могут содержать дополнительные атрибуты:

Наименование	Ограничение длины	Описание
Registration number FSS	10	Регистрационный номер организации-страхователя в ФСС – опционально

Атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом, являются:

Наименование	Ограничение длины	Описание
Common Name	64	Фамилия, имя и отчество (при наличии) владельца сертификата – обязательно
Surname	40	Фамилия владельца сертификата – обязательно
Given name	64	Имя и отчество (при наличии) владельца сертификата – обязательно
Locality	128	Наименование населенного пункта по адресу регистрации владельца сертификата – обязательно
State Or Province	128	Код и наименование субъекта РФ по адресу регистрации владельца сертификата – обязательно
Country	2	RU
Email	255	Адрес электронной почты владельца сертификата
SNILS	11	СНИЛС владельца сертификата – обязательно
INN	12	ИНН владельца сертификата – обязательно

Атрибутами поля идентификационных данных Владельца сертификата – юридического лица, являются:

Наименование	Ограничение длины	Описание
Common Name	64	Наименование организации – обязательно
Organization	64	Наименование организации – обязательно
Street	128	Часть адреса местонахождения организации, включающая наименование улицы, номер дома, корпуса, строения, квартиры, помещения, – обязательно
Locality	128	Наименование населенного пункта по адресу местонахождения организации – обязательно

State Or Province	128	Код и наименование субъекта РФ по адресу местонахождения организации – обязательно
Country	2	RU
Email	255	Адрес электронной почты организации – опционально
OGRN	13	ОГРН организации – обязательно
INN	12	ИНН организации – обязательно (первые два разряда заполняются нулями)

### Сведения об областях применения

В поле Extended Key Usage всех квалифицированных сертификатов включается:

OID	Описание	Примечание
1.3.6.1.5.5.7.3.2	Проверка подлинности клиента	
1.3.6.1.5.5.7.3.4	Защищенная электронная почта	При наличии в поле Subject атрибута Email

Дополнительно в поле Extended Key Usage может быть добавлена одна из следующих совокупностей областей применения:

### Сертификаты для электронных торговых площадок (ЭТП)

OID	Описание	Примечание
1.2.643.6.7	Использование в электронных торговых системах B2B-Center	Указывается в соответствии с нормативными актами ЭТП
1.2.643.6.15	ЭТП Фабрикант.ру	
1.2.643.3.5.10.2.12	Участник, имеющий право на включение сведений в Единый федеральный реестр сведений о фактах деятельности юридических лиц	Указывает на возможность использования сертификата в системе ЕФРСДЮЛ (Федресурс)

### Сертификаты для использования в ИС Росреестра и СМЭВ

OID	Описание	Примечание
1.2.643.100.2.1	Доступ к СМЭВ ЭП-СП	Указывает на возможность доступа к системе СМЭВ от имени должностного лица органа власти, участвующего в межведомственном взаимодействии при оказании государственных и муниципальных услуг

1.2.643.5.1.24.2.X	Объектные идентификаторы пользователей ИС Росреестра	Значение X определяется в соответствии с нормативноправовыми актами Росреестра
1.2.643.3.5.10.2.12	Участник, имеющий право на включение сведений в Единый федеральный реестр сведений о фактах деятельности юридических лиц	Указывает на возможность использования сертификата в системе ЕФРСДЮЛ (Федресурс)

Сертификаты для использования в СМЭВ органами государственной власти и местного самоуправления

OID	Описание	Примечание
1.2.643.100.2.2	Доступ к СМЭВ ЭП-ОВ	Указывает на возможность доступа к системе СМЭВ от имени должностного лица органа власти, участвующего в межведомственном взаимодействии при оказании государственных и муниципальных услуг

Также по соглашению с информационными системами, в которых применяются Сертификаты, могут включаться дополнительные OID.

#### **Доступ к сведениям о статусе сертификата**

1.1 Удостоверяющий центр публикует Реестр отозванных сертификатов по адресам, определенным в расширении «Точки распространения списков отзыва (CRL distribution points)» (OID – 2.5.29.31) Сертификата.

1.2 Информация о прекращении действия или аннулировании Сертификата КЭП вносится в Реестр отозванных сертификатов в течение 30 минут с момента приема заявления на прекращение действия такого Сертификата или наступления иного события, предусмотренного пунктами 8.8.1, 8.8.2 Регламента.

1.3 В случае если дополнение AIA (Authority Information Access, доступ к информации о центрах сертификации) сертификата содержит ссылку на службу OCSP, указанная служба может быть использована для получения актуальной информации о статусе Сертификата.

## Приложение № 8 к Регламенту УЦ ООО «ДИАС-К» РУКОВОДСТВО по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

### Введение

Настоящее «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» (далее – Руководство) разработано в соответствии со следующими нормативно-правовыми актами:

- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи";
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Приказ ФСБ РФ от 09.02.2005 № 66 (ред. от 12.04.2010) "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)".

Руководство предназначено для **обязательного** ознакомления Пользователей Удостоверяющего центра общества с ограниченной ответственностью «ДИАС-К» (далее – УЦ ООО «ДИАС-К») использующих квалифицированную электронную подпись и средства квалифицированной электронной подписи

### 1. Основные термины и определения

**Удостоверяющий центр** - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

**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.

**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.

**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.

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

**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);

**Ключевой носитель** – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

**Ключевой документ** – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию.

**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.

## **2. Организационно-технические меры обеспечения безопасности квалифицированной электронной подписи и средств квалифицированной электронной подписи**

2.1. Помещения, в которых размещаются ПЭВМ со средствами электронной подписи должны обеспечивать конфиденциальность проводимых работ и исключать возможность бесконтрольного проникновения в них посторонних лиц;

2.2. ПЭВМ со средствами электронной подписи должны быть оснащены средствами контроля вскрытия (опечатаны, опломбированы), при выявлении факта несанкционированного вскрытия работа на такой ПЭВМ должна быть прекращена;

2.3. ПЭВМ со средствами электронной подписи должны быть оснащены только лицензионным программным обеспечением, в случае обнаружения посторонних программ, нарушения целостности программного обеспечения, работа на такой ПЭВМ должна быть прекращена;

2.4. На время отсутствия Пользователя аппаратные средства, с которыми осуществляется штатное функционирование средств электронной подписи необходимо отключать от линии связи, а ключевые документы должны быть убраны в опечатываемое хранилище;

2.5. Хранить ключевые документы, средства электронной подписи, соответствующую эксплуатационную и техническую документацию следует в шкафах (ящиках, хранилищах) индивидуального использования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.6. Необходимо предусмотреть отдельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации;

2.7. Использовать автоматизированное рабочее место (АРМ) с установленными средствами электронной подписи необходимо в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации;

2.8. При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 6 символов. В отдельных случаях при невозможности использования парольной защиты, допускается загрузка операционной системы без запроса пароля. При этом должны быть реализованы дополнительные организационно – режимные меры, исключающие несанкционированный доступ к этим АРМ;

2.9. Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными средствами электронной подписи;

2.10. Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам;

2.11. Вхождение в режим конфигурирования BIOS штатными средствами BIOS должно осуществляться только с использованием парольной защиты при длине пароля не менее 6 символов;

2.12. При увольнении или переводе в другое подразделение (на другую должность), изменении функциональных обязанностей сотрудника, имевшего доступ к ключевым документам, должна быть проведена смена ключей электронной подписи.

### **3. Правила работы с квалифицированной электронной подписью и средствами квалифицированной электронной подписи**

3.1. При работе с квалифицированной электронной подписью и средствами электронной подписи Пользователь УЦ ООО «ДИАС-К» **обязан**:

- 3.1.1. не разглашать конфиденциальную информацию, к которой имеется доступ, рубежи ее защиты;
- 3.1.2. соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием средств электронной подписи;
- 3.1.3. не нарушать целостность ключевой информации;
- 3.1.4. сохранять в тайне пин-код для доступа к ключевому носителю;
- 3.1.5. обеспечить условия хранения ключевого носителя, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования и копирования;
- 3.1.6. сохранять в тайне содержание средств электронной подписи;
- 3.1.7. использовать для создания, проверки квалифицированной электронной подписи только сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи;
- 3.1.8. использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены);
- 3.1.9. не допускать использование принадлежащего ему ключа электронной подписи без согласия другими лицами;
- 3.1.10. своевременно обновлять сертификат ключа проверки электронной подписи при истечении его срока действия в соответствии с Регламентом УЦ ООО «ДИАС-К»;
- 3.1.11. не использовать ключ электронной подписи и немедленно обратиться в удостоверяющий центр УЦ ООО «ДИАС-К», выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- 3.1.12. не использовать ключ электронной подписи, сертификат ключа проверки электронной подписи которого аннулирован, приостановлен или прекратил действие;
- 3.1.13. немедленно уведомить удостоверяющий центр о фактах утраты или компрометации электронной подписи, средств электронной подписи и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки такой информации;
- 3.1.14. сдать средства квалифицированной электронной подписи, эксплуатационную и техническую документацию к ним в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи.

3.2. Пользователю УЦ ООО «ДИАС-К» **запрещается**:

- 3.2.1. оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи после ввода ключевой информации либо иной конфиденциальной информации;
- 3.2.2. вносить изменение в программное обеспечение средств электронной подписи;
- 3.2.3. осуществлять несанкционированное копирование ключевых носителей;
- 3.2.4. разглашать содержимое носителей ключевой информации или передавать носители лицам к ним не допущенным;
- 3.2.5. выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- 3.2.6. использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;
- 3.2.7. записывать на ключевые носители постороннюю информацию;
- 3.2.8. вставлять ключевой носитель в устройство считывания при проведении работ, не являющихся штатными процедурами использования средств электронной подписи;

3.2.9. изменять настройки, установленные программой установки средства квалифицированной электронной подписи или администратором в соответствии с технической документацией.

Перечень рекомендаций, приведенных в настоящем документе, не является исчерпывающим. Пользователь удостоверяющего центра УЦ ООО «ДИАС-К» обязан выполнять иные действия, предусмотренные нормативными документами в области защиты информации по предотвращению несанкционированного использования цифровой подписи и средств цифровой подписи. Пользователь УЦ ООО «ДИАС-К» также обязан в полной мере выполнять требования технической документации на используемые средства электронной подписи, и средства криптографической защиты информации.