

ООО «Цифровые системы контроля»

УТВЕРЖДЕН
Приказом ООО «Цифровые системы контроля»
От 10 октября 2013 г. № 3/УЦ

РЕГЛАМЕНТ

Удостоверяющего центра «ЦСК»

по созданию и управлению
квалифицированными сертификатами
ключей проверки электронной подписи
OID 1.2.643.3.157.1.1.3

Редакция № 2

г. Калининград
2013

1. Сведения об Удостоверяющем центре.

Общество с ограниченной ответственностью «Цифровые системы контроля», именуемое в дальнейшем «Удостоверяющий центр «ЦСК», зарегистрировано на территории Российской Федерации в городе Калининград. Свидетельство о государственной регистрации юридического лица серия 39 № 000837451, выдано 14.10.2005 г. межрайонной инспекцией ФНС №9 по г.Калининграду. Основной государственный регистрационный номер (ОГРН) 1053903302584.

Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании Свидетельства об аккредитации удостоверяющего центра № 94 от 10 сентября 2012 г., выданного Минкомсвязи России (федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи), и на основании следующих лицензий:

1. **Лицензия Управления ФСБ РФ по Калининградской области ЛСЗ № 0006020 от 12 сентября 2013 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).**

Реквизиты ООО «Цифровые системы контроля»:

Полное наименование: Общество с ограниченной ответственностью «Цифровые системы контроля»

Юридический адрес: 236016, г.Калининград, Литовский вал, д.36

Почтовый адрес: 236008, г.Калининград, ул. Ленинградская, д.4

Банковские реквизиты:

- Филиал № 7806 ВТБ 24 (ПАО), г. Санкт-Петербург
- БИК 044030811
- Р/с 40702810916380000265
- К/с 30101810300000000811

ИНН/КПП: 3906143236/390601001

ОГРН: 1053903302584

Код по ОКВЭД: 52.48.13, 72.2, 74.84

Код по ОКПО: 78633918

Контактные телефоны, факс, адрес электронной почты:

- тел. (4012) 777-112, факс (4012) 347-401; e-mail: uc@dsyst.com

2. Термины и определения.

В настоящем Регламенте используются термины и определения, установленные Федеральным законом «Об электронной подписи», а также термины и определения их дополняющие и конкретизирующие, а именно:

Администратор Удостоверяющего центра – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по обеспечению создания ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, управлению (выдача, аннулирование, прекращение, приостановление и возобновление действия) сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра и уполномоченный Удостоверяющим центром заверять копии сертификатов ключей проверки электронной подписи на бумажном носителе, выданных Удостоверяющим центром.

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

Доверенное лицо удостоверяющего центра - физическое лицо, являющееся сотрудником Удостоверяющего центра или Центра технического обеспечения (ЦТО) и наделенное Удостоверяющим центром полномочиями по выдаче квалифицированных сертификатов ключей проверки электронной подписи, а также иными полномочиями согласно настоящему Регламенту.

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

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

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

Ключ электронной подписи Удостоверяющего центра – ключ электронной подписи, используемый Удостоверяющим центром для создания сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.

Копия сертификата ключа проверки электронной подписи - документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра и заверенный печатью Удостоверяющего центра. Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи. Структура копии сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

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. Допускается не указывать в сертификате ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат используется для автоматического создания или автоматической проверки электронной подписи.

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

Сертификат ключа проверки электронной подписи - электронный документ, выданный Удостоверяющим центром или доверенным лицом Удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

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

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

Сертификат ключа проверки электронной подписи Удостоверяющего центра – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи Удостоверяющего центра в созданных им сертификатах ключей проверки электронной подписи и списках отозванных сертификатов.

Сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в электронных ответах Службы актуальных статусов сертификатов, содержащих информацию о статусе сертификатов, выданных Удостоверяющим центром.

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

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.

Удостоверяющий центр (УЦ) – общество с ограниченной ответственностью «ЦИФРОВЫЕ СИСТЕМЫ КОНТРОЛЯ», осуществляющее выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи». Удостоверяющий центр с момента аккредитации уполномоченным федеральным органом исполнительной власти Российской Федерации в сфере использования электронной подписи осуществляет создание и выдачу квалифицированных сертификатов ключей проверки электронной подписи.

Центр технического обеспечения (ЦТО) - обособленное подразделение Удостоверяющего центра или действующее на основании агентского договора с Удостоверяющим центром юридическое лицо или ИП, из числа сотрудников которого назначается Доверенное лицо.

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

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

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.

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

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

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

3. Статус Регламента.

3.1. Регламент Удостоверяющего центра «ЦСК» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

3.2. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

3.3. Настоящий Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Сторон, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.

3.4. Настоящий регламент распространяется:

в форме электронного документа:

- по адресу: URL=<http://www.dsyst.com>

в форме документа на бумажном носителе:

- при подаче Заявления о присоединении к Регламенту (за вознаграждение, установленное Прейскурантом на услуги Удостоверяющего центра).

4. Общие положения.

4.1. Присоединение к Регламенту.

4.1.1. Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления заинтересованным лицом в Удостоверяющий центр Заявления о присоединении к Регламенту по форме Приложения № 1 настоящего Регламента.

4.1.2. С момента регистрации Заявления о присоединении к Регламенту в Удостоверяющем центре лицо, подавшее Заявление, считается присоединившемся к Регламенту и является Стороной Регламента.

4.1.3. Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации Заявления о присоединении к Регламенту.

4.1.4. Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении в реестре Удостоверяющего центра. Лицо,

присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

4.1.5. После присоединения к Регламенту Удостоверяющий центр и Сторона, присоединившаяся к Регламенту, вступают в соответствующие договорные отношения на неопределённый срок.

4.2. Порядок расторжения Регламента.

4.2.1. Действие настоящего Регламента может быть прекращено по инициативе одной из Сторон в следующих случаях:

- по желанию одной из Сторон;
- при нарушении одной из Сторон условий настоящего Регламента.

4.2.2. В случае расторжения Регламента инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за тридцать календарных дней до даты расторжения Регламента. Регламент считается расторгнутым после выполнения Сторонами своих обязательств и проведения взаиморасчетов согласно условиям Регламента.

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

4.3. Изменение (дополнение) Регламента.

4.3.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

4.3.2. Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений (дополнений) на сайте Удостоверяющего центра по адресу – <http://www.dsyst.com>.

4.3.3. Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении двух месяцев с даты размещения указанных изменений и дополнений в Регламенте на сайте Удостоверяющего центра по адресу - <http://www.dsyst.com>.

4.3.4. 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.

4.3.5. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона Регламента имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренном п.4.2. настоящего Регламента.

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

4.4. Применение Регламента.

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

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

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

5. Предоставление информации.

5.1. Удостоверяющий центр осуществляет свою деятельность в качестве аккредитованного удостоверяющего центра на основании решения Минкомсвязи России, являющегося федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. С информацией по аккредитации Удостоверяющего центра Сторона, присоединившаяся к Регламенту, может ознакомиться на официальном сайте Минкомсвязи России.

5.2. Удостоверяющий Центр предоставляет Стороне, присоединившейся к Регламенту, по ее требованию:

- копию лицензии на осуществление профессиональной деятельности по распространению шифровальных (криптографических средств);
- копию лицензии на осуществление профессиональной деятельности по техническому обслуживанию шифровальных (криптографических средств);
- копию лицензии на осуществление профессиональной деятельности на предоставление услуг в области шифрования информации.

5.3. Удостоверяющий центр вправе запросить, а Сторона, присоединившаяся к Регламенту, обязана предоставить Удостоверяющему центру документы, подтверждающие следующую информацию:

Для юридических лиц:

- нотариально заверенную копию учредительных документов организации;
- выписку из Единого государственного реестра юридических лиц, полученную не ранее чем за один месяц до момента запроса Удостоверяющего центра, или ее нотариально заверенную копию;
- нотариально заверенную копию свидетельства о постановке на учет в налоговом органе заявителя;
- нотариально заверенную копию свидетельства о внесении записи о юридическом лице в Единый государственный реестр юридических лиц;
- копии протоколов, либо иных документов, о назначении уполномоченных лиц организации (в соответствии с учредительными документами организации) и/или надлежащим образом оформленные доверенности;
- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность - для тех лиц, которые указываются в сертификатах ключей проверки электронной подписи наряду с указанием наименования юридического лица (либо нотариально заверенные копии этих документов);
- иные документы, установленные Регламентом Удостоверяющего центра, а также дополнительные документы по усмотрению Удостоверяющего центра.

Для физических лиц:

- документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность (либо нотариально заверенные копии этих документов);
- страховое свидетельство государственного пенсионного страхования заявителя;

- иные документы, установленные Регламентом Удостоверяющего центра, а также дополнительные документы по усмотрению Удостоверяющего центра.

6. Права и обязанности сторон.

6.1. Удостоверяющий центр обязан:

6.1.1. Предоставить Пользователю Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме.

6.1.2. Использовать для создания ключа электронной подписи Удостоверяющего центра и формирования электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

6.1.3. Использовать ключ электронной подписи Удостоверяющего центра только для электронной подписи создаваемых им сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.

6.1.4. Принять меры по защите ключа электронной подписи Удостоверяющего центра от несанкционированного доступа.

6.1.5. Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Калининград. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

6.1.6. Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным Удостоверяющим центром.

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

6.1.8. Создать сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению на создание сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

6.1.9. Обеспечить уникальность серийных номеров создаваемых сертификатов ключей проверки электронной подписи.

6.1.10. Обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах ключей проверки электронной подписи Пользователей Удостоверяющего центра.

6.1.11. Обеспечить сохранение в тайне созданного ключа электронной подписи Пользователя Удостоверяющего центра.

6.1.12. Прекратить, приостановить и возобновить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по соответствующему заявлению на прекращение, приостановление и возобновление действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

6.1.13. Прекратить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра, если истек установленный срок, на который действие данного сертификата было приостановлено.

6.1.14. Прекратить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра.

6.1.15. Официально уведомить об аннулировании, прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации списка отозванных сертификатов.

6.1.16. Публиковать актуальный список отозванных сертификатов на сайте Удостоверяющего центра в ресурсе: <http://www.dsyst.com> в течение 1 часа с момента аннулирования, прекращения, приостановления и возобновления действия сертификата ключа проверки электронной подписи.

6.2. Сторона, присоединившаяся к Регламенту, обязана:

6.2.1. Известить Удостоверяющий центр об изменениях в документах, приведенных в п.5.3. и по требованию Удостоверяющего центра предоставить их в течение 5-ти рабочих дней с момента регистрации изменений.

6.2.2. С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра по адресу <http://www.dsyst.com> за сведениями об изменениях и дополнениях в Регламент.

6.2.3. Пользователь Удостоверяющего центра обязан:

6.2.3.1. Хранить в тайне ключи электронных подписей, принимать все возможные меры для предотвращения их потери, раскрытия, искажения и несанкционированного использования.

6.2.3.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

6.2.3.3. Не применять ключ электронной подписи, при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

6.2.3.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

6.2.3.5. Немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия сертификата ключа проверки электронной подписи в случае потери, нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

6.2.3.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено

6.2.3.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

6.2.3.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

6.2.3.9. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи только сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

6.3. Удостоверяющий центр имеет право:

6.3.1. Отказать пользователю в регистрации в Удостоверяющем центре в случае ненадлежащего оформления необходимых регистрационных документов.

6.3.2. Отказать в изготовлении сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на изготовление сертификата ключа проверки электронной подписи, а также в случае не предоставления и/или ненадлежащего предоставления документов, установленных п. 5.3 настоящего Регламента.

6.3.3. Отказать в прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления на прекращение, приостановление и возобновление действия сертификата ключа проверки электронной подписи.

6.3.4. Отказать в прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификату.

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

6.4. Пользователь Удостоверяющего центра имеет право:

6.4.1. Получить копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную Удостоверяющим центром.

6.4.2. Применять сертификат ключа проверки электронной подписи Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в сертификатах ключей проверки электронных подписей, созданных Удостоверяющим центром.

6.4.3. Применять список отозванных сертификатов ключей проверки электронных подписей, созданный Удостоверяющим центром, для установления статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

6.4.4. Применять для хранения ключа электронной подписи ключевой носитель, поддерживаемый средством электронной подписи, определённым сертификатом ключа проверки электронной подписи, соответствующим ключу электронной подписи.

6.4.5. Обратиться в Удостоверяющий центр с заявлениями на выполнение Удостоверяющим центром действий, установленных настоящим Регламентом.

6.4.6. Пользоваться сервисами Службы актуальных статусов сертификатов и Службы штампов времени Удостоверяющего центра.

7. Порядок предоставления и пользования услугами Удостоверяющего центра

7.1. Создание сертификата ключа проверки электронной подписи

Удостоверяющий центр осуществляет создание сертификатов ключей проверки электронной подписи только тем лицам, которые присоединились к настоящему Регламенту и являются Стороной настоящего Регламента.

Создание сертификата ключа проверки электронной подписи осуществляется на основании заявления на создание сертификата ключа проверки электронной подписи. Форма заявления на создание сертификата ключа проверки электронной подписи приведена в Приложении № 2 настоящего Регламента.

В случае создания сертификата ключа проверки электронной подписи юридическому лицу наряду с указанием в сертификате наименования юридического лица должно указываться физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Указанная доверенность должна предоставляться заявителем вместе с заявлением на создание сертификата ключа проверки электронной подписи, оформляться по форме Приложения № 3 настоящего Регламента и быть действительной на момент создания сертификата ключа проверки электронной подписи. Если ключи электронной подписи и сертификат ключа проверки электронной подписи юридического лица будут использоваться для автоматического создания электронных подписей, то физическое лицо может не указываться в сертификате ключа проверки электронной подписи.

Предоставление заявительных документов для создания сертификата ключа проверки электронной подписи, а также получение сформированных Удостоверяющим центром ключа электронной подписи и сертификата ключа проверки электронной подписи может быть осуществлено:

- для юридического лица:
 - физическим лицом, которое указывается в сертификате наряду с наименованием юридического лица;
 - физическим лицом на основании доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи, оформленной по форме Приложения № 4 к настоящему Регламенту;

- для физического лица:
 - непосредственно этим физическим лицом;
 - физическим лицом на основании нотариально заверенной доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи, оформленной по форме Приложения № 4 к настоящему Регламенту.

Администратор Удостоверяющего центра на основе предоставленных заявительных документов выполняет действия по формированию ключа электронной подписи и созданию сертификата ключа проверки электронной подписи. Ключ электронной подписи и сертификат ключа проверки электронной подписи записываются на предоставляемый заявителем ключевой носитель.

Администратор Удостоверяющего центра передает сформированный ключевой носитель заявителю и распечатывает на бумажном носителе информацию, содержащуюся в созданном сертификате ключа проверки электронной подписи, представленную в виде копии сертификата, оформленной по форме Приложения № 10. Заявитель под расписку ознакомляется с информацией из сертификата ключа проверки электронной подписи.

Дополнительно, по согласованию с заявителем, Администратором Удостоверяющего центра сообщается ключевая фраза, используемая для аутентификации Пользователя Удостоверяющего центра при выполнении регламентных процедур, возникающих при нарушении конфиденциальности ключевых документов Пользователя Удостоверяющего центра.

Создание и выдача сертификатов ключей проверки электронной подписи Удостоверяющим центром осуществляется в день прибытия заявителя. День прибытия заявителя согласовывается с Администратором Удостоверяющего центра. Удостоверяющий центр вправе отказать в создании сертификатов по заявлениям, поступившим в Удостоверяющий центр без согласования дня прибытия заявителя.

7.2. Прекращение действия сертификата ключа проверки электронной подписи

Удостоверяющий центр прекращает действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в следующих случаях:

- при прекращении действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту, по усмотрению Удостоверяющего центра;
- по истечении срока, на который действие сертификата было приостановлено;
- по заявлению владельца сертификата ключа проверки электронной подписи;
- в связи с аннулированием сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу.
- по истечении срока действия сертификата ключа проверки электронной подписи;
- при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи;

В случае прекращения действия настоящего Регламента, истечения срока, на который действие сертификата было приостановлено, по заявлению владельца сертификата, по решению суда, вступившего в законную силу Удостоверяющий центр официально уведомляет владельца сертификата и всех Пользователей Удостоверяющего центра о прекращении действия сертификата ключа проверки электронной подписи не позднее одного рабочего дня с момента наступления описанного события.

Официальным уведомлением о факте прекращения действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого прекращено, и изданного не ранее времени наступления произошедшего случая. Временем прекращения действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящиеся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL Distribution Point сертификата ключа проверки электронной подписи.

В случае прекращения действия сертификата ключа проверки электронной подписи по истечению срока его действия временем прекращения действия сертификата ключа проверки электронной подписи признается время, хранящееся в поле `notAfter` поля `Validity` сертификата ключа проверки электронной подписи. В этом случае информация о сертификате, действие которого прекращено, в список отозванных сертификатов не заносится.

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра временем прекращения действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра признается время нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, фиксирующееся Удостоверяющим центром. При этом информация о сертификате ключа проверки электронной подписи Пользователя Удостоверяющего центра в список отозванных сертификатов не заносится.

7.2.1. Прекращение действия сертификата ключа проверки электронной подписи по заявлению его владельца

Подача заявления в Удостоверяющий центр на прекращение действия сертификата ключа проверки электронной подписи может быть осуществлена посредством почтовой или курьерской связи по форме Приложения № 5 настоящего Регламента.

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 не позднее рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в прекращении действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения Администратор Удостоверяющего центра осуществляет прекращение действия сертификата ключа проверки электронной подписи.

7.3. Приостановление действия сертификата ключа проверки электронной подписи

Удостоверяющий центр приостанавливает действие сертификата ключа проверки электронной подписи в следующих случаях:

- по заявлению владельца сертификата ключа проверки электронной подписи;
- по заявке владельца сертификата ключа проверки электронной подписи в устной форме в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению Удостоверяющего центра.

Действие сертификата ключа проверки электронной подписи приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата ключа проверки электронной подписи составляет 15 (Пятнадцать) дней.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи действие этого сертификата не будет возобновлено, то данный сертификат прекращает своё действие.

Официальным уведомлением о факте приостановления действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, и изданного не ранее времени наступления произошедшего случая. Временем приостановления действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL Distribution Point сертификата ключа проверки электронной подписи.

7.3.1. Приостановление действия сертификата ключа проверки электронной подписи по заявлению его владельца

Подача заявления в Удостоверяющий центр на приостановление действия сертификата ключа проверки электронной подписи может быть осуществлена посредством почтовой или курьерской связи по форме Приложения № 6 настоящего Регламента.

После получения Удостоверяющим центром заявления на приостановление действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в приостановление действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения Администратор Удостоверяющего центра осуществляет приостановление действия сертификата ключа проверки электронной подписи.

7.3.2. Приостановление действия сертификата ключа проверки электронной подписи по заявке в устной форме его владельца

Приостановление действия сертификата ключа проверки электронной подписи по заявке в устной форме осуществляется исключительно при нарушении конфиденциальности ключа электронной подписи или подозрении в нарушении конфиденциальности ключа электронной подписи Пользователя Удостоверяющего центра.

Заявка подается в Удостоверяющий центр по телефону.

Пользователь Удостоверяющего центра должен сообщить Администратору Удостоверяющего центра следующую информацию:

- идентификационные данные, содержащиеся в сертификате ключа проверки электронной подписи, действие которого необходимо приостановить;

- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется приостановить;
- ключевую фразу Пользователя Удостоверяющего центра (ключевая фраза определяется в процессе изготовления сертификата ключа проверки электронной подписи).

Заявка на приостановление действия сертификата принимается Удостоверяющим центром только в случае положительной аутентификации Пользователя Удостоверяющего центра (совпадения ключевой фразы, сообщенной Пользователем Удостоверяющего центра по телефону, и ключевой фразы, хранящейся в Удостоверяющем центре).

После принятия заявки Администратор Удостоверяющего центра принимает решение о приостановлении действия сертификата ключа проверки электронной подписи, которое должно быть осуществлено в течение рабочего дня поступления данной заявки.

В случае отказа в приостановлении действия сертификата ключа проверки электронной подписи Пользователь Удостоверяющего центра уведомляется об этом с указанием причины отклонения заявки.

При принятии положительного решения Администратор Удостоверяющего центра приостанавливает действие сертификата ключа проверки электронной подписи до окончания срока действия ключа электронной подписи, соответствующего данному сертификату.

Не позднее 5 (пяти) рабочих дней с момента приостановления действия сертификата ключа проверки электронной подписи владелец сертификата должен предоставить в Удостоверяющий центр заявление на прекращение действия сертификата (в том случае, если факт нарушения конфиденциальности ключа электронной подписи подтвердился), либо заявление на возобновление действия сертификата (в том случае, если нарушения конфиденциальности ключа электронной подписи не было).

7.3.3. Приостановление действия сертификата ключа проверки электронной подписи по решению Удостоверяющего центра

Удостоверяющий центр вправе приостановить действие сертификата ключа проверки электронной подписи в случаях нарушения конфиденциальности или подозрения в нарушении конфиденциальности соответствующего ключа электронной подписи в том случае, если владельцу сертификата ключа проверки электронной подписи не было известно о возможном факте нарушения конфиденциальности ключей, а также в случаях неисполнения владельцем сертификата ключа проверки электронной подписи обязательств по настоящему Регламенту.

После приостановления действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра сообщает владельцу сертификата ключа проверки электронной подписи о наступлении события, повлекшего приостановление действия сертификата, и уведомляет его о том, что действие сертификата приостановлено.

7.4. Возобновление действия сертификата ключа проверки электронной подписи

Удостоверяющий центр возобновляет действие сертификата ключа проверки электронной подписи только по заявлению его владельца и только в том случае, если действие сертификата ключа проверки электронной подписи было приостановлено.

Подача заявления в Удостоверяющий центр на возобновление действия сертификата ключа проверки электронной подписи может быть осуществлена посредством почтовой или курьерской связи по форме Приложения № 7 настоящего Регламента.

После получения Удостоверяющим центром заявления на возобновление действия сертификата ключа проверки электронной подписи Администратор Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на возобновление действия сертификата должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в возобновлении действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения Администратор Удостоверяющего центра осуществляет возобновление действия сертификата ключа проверки электронной подписи.

Официальным уведомлением о факте возобновления действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, не содержащего сведения о сертификате, действие которого было возобновлено, и изданного не ранее времени предоставления заявления на возобновление действия сертификата. Временем возобновления действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле `thisUpdate` списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL Distribution Point.

7.5. Получение информации о статусе сертификата ключа проверки электронной подписи

Получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром осуществляется на основании заявления Стороны, присоединившейся к Регламенту. Данное заявление оформляется по форме Приложения № 8 настоящего Регламента и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

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

Предоставление заявителю справки о статусе сертификата ключа проверки электронной подписи должно быть осуществлено не позднее 10 (Десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

7.6. Проверка подлинности электронной подписи в электронном документе

По желанию Стороны, присоединившейся к Регламенту, Удостоверяющий центр осуществляет проведение экспертных работ по проверке подлинности электронной подписи в электронном документе.

В том случае, если формат представления электронной подписи (формат представления электронного документа с электронной подписью) соответствует стандарту криптографических сообщений Cryptographic Message Syntax (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.

Для проверки подлинности электронной подписи в электронных документах Сторона, присоединившаяся к Регламенту, подает заявление в Удостоверяющий центр по форме, приведенной в Приложении № 9 настоящего Регламента.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные владельца сертификата, электронную подпись которого необходимо проверить в электронном документе;
- дата и время формирования электронной подписи электронного документа;

– дата и время, на момент наступления которых требуется проверить подлинность электронной подписи (в том случае, если информация о дате и времени подписания электронного документа отсутствует).

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

– сертификат ключа проверки электронной подписи, с использованием которого необходимо проверить подлинность 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).

Проведение работ по проверке подлинности электронной подписи в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

Результатом проведения работ по проверке подлинности электронной подписи в электронном документе является заключение Удостоверяющего центра.

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- данные, предоставленные комиссии для проведения проверки.
- результат проверки электронной подписи электронного документа.

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

Срок проведения работ по проверке подлинности электронной подписи в одном электронном документе и предоставлению заявителю заключения по выполненной проверке составляет 10 (Десять) рабочих дней с момента поступления заявления в Удостоверяющий центр.

В том случае, если формат представления электронной подписи (формат представления электронного документа с электронной подписью) не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то проведение экспертных работ по проверке подлинности электронной подписи осуществляется в рамках заключения отдельного договора между Удостоверяющим центром и Стороной, присоединившейся к Регламенту. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором.

7.7. 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://www.dsyst.com/ocsp63/ocsp.srf>. Указанный адрес заносится в расширение Authority Information Access (AIA) создаваемых Удостоверяющим центром 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://www.dsyst.com/tsp63/tsp.srf>.

8. Вознаграждение Удостоверяющего центра. Сроки и порядок расчетов.

8.1. Вознаграждение Удостоверяющего центра по настоящему Регламенту устанавливается в соответствии с Прейскурантом на услуги Удостоверяющего центра. Ознакомиться с действующим прейскурантом можно в офисе Удостоверяющего центра или на сайте по адресу <http://www.dsyst.com>.

8.2. Оплата услуг Удостоверяющего центра осуществляется на основании счета на оплату в российских рублях в безналичном порядке или иным способом, предусмотренным законодательством Российской Федерации.

8.3. По факту изготовления сертификатов ключей подписей Удостоверяющий центр выставляет Стороне, присоединившейся к Регламенту, счет на оплату изготовленных сертификатов ключей подписей. Сторона, присоединившаяся к Регламенту, обязуется оплатить таковой счет в течение 3 (Трех) банковских дней с момента его получения.

8.4. Изготовление сертификатов ключей подписей, вызванных внеплановой сменой ключей Пользователей УЦ, осуществляется Удостоверяющим центром безвозмездно.

9. Ответственность сторон.

9.1. В случае невыполнения Стороной, присоединившейся к Регламенту, обязательств по оплате изготовленных сертификатов ключей электронных подписей, изложенных в разделе 8 настоящего Регламента, Удостоверяющий центр имеет право приостановить действие изготовленных сертификатов ключей подписей.

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

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

9.4. Удостоверяющий центр не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях Пользователя Удостоверяющего центра.

9.5. Удостоверяющий центр несет ответственность за убытки при использовании созданного Удостоверяющим центром ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра только в случае, если данные убытки возникли по причине нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра.

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

10. Разрешение споров.

10.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к Регламенту.

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

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

10.4. Сторона, получившая от другой Стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

10.5. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде города Калининграда.

11. Сроки действия ключевых документов и структура сертификатов ключей подписей.

11.1. Сроки действия ключевых документов

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

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

Срок действия сертификата ключа проверки электронной подписи Удостоверяющего центра не превышает 10 (десять) лет. Время начала периода действия сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

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 10 (десять) 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 10 (десять) 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.

11.1.2. Сроки действия ключевых документов Пользователя Удостоверяющего центра

Срок действия ключа электронной подписи пользователя Удостоверяющего центра составляет 1 (Один) год.

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

Срок действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (клиентский сертификат ключа подписи) не превышает 10 (десять) лет. Время начала периода действия сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно.

11.2. Структура квалифицированного сертификата ключа проверки электронной подписи Удостоверяющего центра.

| Название | Описание | Содержание |
|---------------------------------|--|--|
| Базовые поля сертификата | | |
| Version | Версия | V3 |
| Serial Number | Серийный номер | Уникальный серийный номер сертификата |
| Signature Algorithm | Алгоритм ключа проверки электронной подписи | ГОСТ Р 34.10-2001 |
| Issuer | Издатель сертификата | CN = УЦ ЦСК OU = Удостоверяющий центр O = ООО «ЦСК» L = Калининград S = 39 Калининградская область C = RU E = uc@dsyst.com ИНН = 003906143236 ОГРН = 1053903302584 |
| Validity Period | Срок действия сертификата | Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT |
| Subject | Владелец сертификата | CN = УЦ ЦСК OU = Удостоверяющий центр O = ООО «ЦСК» L = Калининград S = 39 Калининградская область C = RU E = uc@dsyst.com ИНН = 003906143236 ОГРН = 1053903302584 |
| Public Key | Открытый ключ | Открытый ключ (алгоритм ГОСТ Р 34.10-2001) |
| Issuer Signature Algorithm | Алгоритм подписи издателя сертификата | ГОСТ Р 34.11/34.10-2001 |
| Issuer Sign | ЭП издателя сертификата | Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 |
| Расширения сертификата | | |
| SubjectSignTool | Наименование средства ЭП, используемого владельцем сертификата | Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011 |
| IssuerSignTool | Средства электронной подписи и УЦ издателя | Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011 |
| Key Usage (critical) | Использование ключа | Неотрекаемость, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL) |
| Basic Constraints (critical) | Основные ограничения использования | Сертификат удостоверяющего центра |
| Subject Key Identifier | Идентификатор ключа владельца сертификата | Идентификатор ключа электронной подписи Удостоверяющего центра, соответствующего данному сертификату |
| Certificate Policies | Политики сертификации | Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011 |
| CA Version | Версия ЦС | Версия сертификата Удостоверяющего центра |

11.3. Структура квалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра.

| Название | Описание | Содержание |
|---------------------------------|--|--|
| Базовые поля сертификата | | |
| Version | Версия | V3 |
| Serial Number | Серийный номер | Уникальный серийный номер сертификата |
| Signature Algorithm | Алгоритм подписи | ГОСТ Р 34.11/34.10-2001 |
| Issuer | Издатель сертификата | CN = УЦ ЦСК OU = Удостоверяющий центр O = ООО «ЦСК» L = Калининград S = 39 Калининградская область C = RU E = uc@dsyst.com ИНН = 003906143236 ОГРН = 1053903302584 |
| Validity Period | Срок действия сертификата | Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT |
| Subject | Владелец сертификата | CommonName = Общее имя = Фамилия, Имя, Отчество или псевдоним OrganizationUnit = Подразделение Organization = Организация Locality = Город State = Область/Субъект Федерации Country = Страна = RU Email = Электронная почта ИНН, ОГРН, СНИЛС |
| Public Key | Открытый ключ | Открытый ключ (ГОСТ Р 34.11/34.10-2001) |
| Issuer Signature Algorithm | Алгоритм подписи издателя сертификата | ГОСТ Р 34.11/34.10-2001 |
| Issuer Sign | ЭП издателя сертификата | Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 |
| Расширения сертификата | | |
| Key Usage (critical) | Использование ключа | Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных |
| Extended Key Usage | Улучшенный ключ | Пользователь Центра Регистрации - (1.2.643.2.2.34.6) Проверка подлинности клиента - (1.3.6.1.5.5.7.3.2) Защищенная электронная почта - (1.3.6.1.5.5.7.3.4) |
| Subject Key Identifier | Идентификатор ключа субъекта | Идентификатор ключа подписи владельца сертификата |
| Authority Key Identifier | Идентификатор ключа центра сертификации | Идентификатор ключа подписи Удостоверяющего центра, которым подписан данный сертификат |
| CRL Distribution Point | Точка распространения списка отозванных сертификатов | URL= http://www.dsyst.com |
| Authority Information Access | Доступ к информации о центрах сертификации | URL адреса web-приложения Службы актуальных статусов сертификатов. Адреса, по которым Удостоверяющий центр опубликовал Сертификат Удостоверяющего центра. |
| Private Key Validity Period | Срок действия ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи | Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC; Действителен по (notAfter): дд.мм.гггг чч:мм:сс UTC |
| Certificate Policies | Политики сертификата | Класс средств ЭП |
| SubjectSignTool | Наименование средства ЭП, используемое владельцем сертификата | Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011 |
| IssuerSignTool | Наименование средств ЭП и средств УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, сертификата, а также реквизиты документов, подтверждающих соответствие указанных средств требованиям, установленным 63-ФЗ | Заполняется в соответствии с приказом ФСБ России № 795 от 27.12.2011 |

11.4. Структура списка отозванных сертификатов (CRL) Удостоверяющего центра.

| Название | Описание | Содержание |
|--|------------------------------------|--|
| Базовые поля списка отозванных сертификатов | | |
| Version | Версия | V2 |
| Issuer | Издатель СОС | CN = УЦ ЦСК OU = Удостоверяющий центр O = ООО «ЦСК» L = Калининград S = 39 Калининградская область C = RU E = uc@dsyst.com ИНН = 003906143236 ОГРН = 1053903302584 |
| 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 (Reason Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия |
| signatureAlgorithm | Алгоритм подписи | ГОСТ Р 34.11/34.10-2001 |
| Issuer Sign | Подпись издателя СОС | Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 |
| Расширения списка отозванных сертификатов | | |
| Authority Key Identifier | Идентификатор ключа издателя | Идентификатор ключа подписи Удостоверяющего центра, на котором подписан СОС |
| CA Version | Версия сертификата издателя | Версия сертификата Удостоверяющего центра |
| CRL Number | Номер СОС | Порядковый номер СОС |
| CRL Next Publish | Следующая публикация СОС | дд.мм.гггг чч:мм:сс GMT |

11.5. Сертификат ключа подписи пользователя Удостоверяющего центра (серверный сертификат) в расширении Extended Key Usage или Application Policy должен содержать, включая, но не ограничиваясь, следующие области использования:

- Проверка подлинности сервера (1.3.6.5.5.7.3.1).

11.6. Сертификат ключа подписи пользователя Удостоверяющего центра с поддержкой сервисов Службы актуальных статусов сертификатов и Службы штампов времени в расширении Extended Key Usage или Application Policy должен содержать, включая, но не ограничиваясь, следующие области использования:

- Пользователь Центра регистрации, HTTP, TLS client (1.2.643.2.2.34.6);
- Проверка подлинности клиента (1.3.6.5.5.7.3.2);
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4);
- Пользователь службы актуальных статусов (1.2.643.2.2.34.26);
- Пользователь службы штампов времени (1.2.643.2.2.34.25).

11.7. Дополнительно в выдаваемые сертификаты ключей проверки электронной подписи могут быть занесены иные поля и расширения по усмотрению Удостоверяющего центра.

12. Дополнительные положения.

12.1. Плановая смена ключей Удостоверяющего центра

Плановая смена ключа электронной подписи и соответствующего ему сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется не ранее, чем через 1 год и не позднее, чем через 1 год 3 месяца после начала действия ключа проверки электронной подписи Удостоверяющего центра.

Процедура плановой смены ключей Удостоверяющего центра осуществляется в следующем порядке:

- Удостоверяющий центр генерирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Удостоверяющий центр создает новый сертификат ключа проверки электронной подписи.

Уведомление пользователей о проведении смены ключей Удостоверяющего центра осуществляется посредством электронной почты.

Старый ключ электронной подписи Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого ключа электронной подписи Удостоверяющего центра.

12.2. Нарушение конфиденциальности ключевых документов Удостоверяющего центра, внеплановая смена ключей Удостоверяющего центра

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификат ключа проверки Удостоверяющего центра прекращает свое действие (аннулируется). Все сертификаты, подписанные с использованием ключа Удостоверяющего центра, конфиденциальность которого нарушена, также прекращают свое действие (считаются аннулированными).

Уведомление Пользователей УЦ о нарушении конфиденциальности ключа подписи Удостоверяющего центра осуществляется посредством размещения данной информации на сайте Удостоверяющего центра <http://www.dsyst.com> и рассылки Пользователям Удостоверяющего центра соответствующего сообщения по электронной почте.

После аннулирования сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется процедура внеплановой смены ключей Удостоверяющего центра. Процедура внеплановой смены ключей Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра (пункт 12.1 настоящего Регламента).

Все подписанные с использованием аннулированного ключа Удостоверяющего центра и действовавшие на момент нарушения конфиденциальности ключа Удостоверяющего центра сертификаты ключей проверки электронных подписей, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

12.3. Нарушение конфиденциальности ключевых документов Пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе нарушения конфиденциальности своего ключа электронной подписи.

В случае нарушения конфиденциальности ключа электронной подписи или угрозы такого нарушения Пользователь связывается с Удостоверяющим центром по телефону и

приостанавливает действие сертификата, соответствующего скомпрометированному ключу, посредством подачи заявления на приостановление действия сертификата в устной форме.

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

12.4. Конфиденциальность информации.

12.4.1. Типы конфиденциальной информации.

12.4.1.1. Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключей электронных подписей Пользователей Удостоверяющего центра.

12.4.1.2. Персональная и корпоративная информация о Пользователях Удостоверяющего центра, не являющаяся частью сертификата ключа проверки электронной подписи, считается конфиденциальной.

12.4.2. Типы информации, не являющейся конфиденциальной.

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

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

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

12.4.2.4. Персональные данные, включаемые в сертификаты ключей подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

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

12.4.3. Исключительные полномочия Удостоверяющего центра.

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

12.5. Хранение сертификатов ключей проверки электронных подписей в Удостоверяющем Центре

Сертификат ключа проверки электронной подписи хранится в Удостоверяющем Центре в течение всего периода его действия и 5 (Пять) лет после прекращения его действия. По истечении указанного срока хранения сертификаты ключей проверки электронных подписей переводятся в режим архивного хранения.

12.6. Прекращение оказания услуг Удостоверяющим центром

12.6.1. В случае расторжения Регламента одной из Сторон действие всех сертификатов ключей проверки электронных подписей, владельцами которых является Пользователь УЦ - Сторона Регламента, прекращается (сертификаты аннулируются).

12.7. Форс-мажор.

12.7.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение

явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

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

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

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

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

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

13. Список приложений.

13.1. Приложение №1. Форма Заявления о присоединении к Регламенту Удостоверяющего центра «ЦСК» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи.

13.2. Приложение №2. Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра «ЦСК».

13.3. Приложение №3. Форма доверенности Пользователя Удостоверяющего центра «ЦСК» на осуществление действий в рамках Регламента Удостоверяющего центра «ЦСК».

13.4. Приложение №4. Форма доверенности на сдачу документов и получение ключей электронной подписи и сертификата ключа электронной подписи Пользователя Удостоверяющего центра «ЦСК».

13.5. Приложение №5. Форма заявления на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра «ЦСК».

13.6. Приложение №6. Форма заявления на приостановление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра «ЦСК».

13.7. Приложение №7. Форма заявления на возобновление действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра «ЦСК».

13.8. Приложение №8. Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром «ЦСК».

13.9. Приложение №9. Форма заявления на подтверждение подлинности электронной подписи в электронном документе.

13.10. Приложение №10. Форма сертификата (копии сертификата) ключа проверки электронной подписи на бумажном носителе.

Для юридических лиц

Заявление
о присоединении к Регламенту
Удостоверяющего центра «ЦСК»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи

_____ (наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра «ЦСК» ООО «Цифровые системы контроля» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, условия которого определены ООО «Цифровые системы контроля» и опубликованы на сайте Удостоверяющего центра «ЦСК» по адресу <http://www.dsyst.com>.

С Регламентом Удостоверяющего центра ООО «ЦСК» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Руководитель организации _____ (_____)
(подпись) (Ф.И.О.)

М.П.

« _____ » _____ 20__ г.

Для физических лиц

Заявление
о присоединении к Регламенту
Удостоверяющего центра «ЦСК»
по созданию и управлению квалифицированными сертификатами
ключей проверки электронной подписи

Я, _____
(фамилия, имя, отчество)

(серия и номер паспорта

кем и когда выдан)

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра «ЦСК» условия которого определены ООО «Цифровые системы контроля» и опубликованы на сайте Удостоверяющего центра «ЦСК» по адресу <http://www.dsyst.com>
С Регламентом Удостоверяющего центра «ЦСК» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

_____ (_____)
(подпись) (Ф.И.О.)

« ____ » _____ 20__ г.

Приложение №2
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на изготовление сертификата ключа проверки
электронной подписи Пользователя)

Для юридических лиц

Заявление
на создание квалифицированного сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра «ЦСК»

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

_____ (фамилия, имя, отчество)

действующего на основании _____

в связи с _____
(причина изготовления сертификата)

Просит сформировать ключи подписи и изготовить сертификат ключа подписи своего
уполномоченного представителя – Пользователя Удостоверяющего центра «ЦСК»

_____ (фамилия, имя, отчество)
Паспорт _____ выдан _____
(серия и номер паспорта) (орган выдавший паспорт)
_____ от _____
(орган выдавший паспорт) (когда выдан паспорт)

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

| | |
|-----------------------------|--|
| Должность | |
| Фамилия (псевдоним) | |
| Имя | |
| Отчество | |
| Наименование подразделения | |
| Наименование организации | |
| Адрес | |
| ИНН | |
| ОГРН | |
| СНИЛС | |
| Город | |
| Область | |
| Страна | RU |
| Адрес электронной почты | |
| Области использования ключа | Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации (1.2.643.2.2.34.6) |

Настоящим _____
(фамилия, имя, отчество)

Соглашается с обработкой своих персональных данных Удостоверяющим центром «ЦСК» и
признает, что персональные данные, заносимые в сертификаты ключей проверки электронной
подписи, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

Руководитель организации _____ (_____)
(фамилия, инициалы)

М.П.

Приложение №2
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на изготовление сертификата ключа подписи Пользователя)

Для физических лиц

Заявление
на создание квалифицированного сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра «ЦСК»

Я, _____
(фамилия, имя, отчество)

Паспорт _____ выдан _____
(серия и номер паспорта) (орган выдавший паспорт)

_____ от _____
(орган выдавший паспорт) (когда выдан паспорт)

Прошу сформировать ключи подписи и изготовить сертификат ключа подписи Пользователя Удостоверяющего центра «ЦСК» в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

| | | |
|-----------------------------|---------------------------------|---------------------|
| Фамилия (псевдоним) | | |
| Имя | | |
| Отчество | | |
| ИНН | | |
| СНИЛС | | |
| Город | | |
| Область | | |
| Страна | | |
| Адрес электронной почты | | |
| Области использования ключа | Проверка подлинности клиента | (1.3.6.1.5.5.7.3.2) |
| | Защищенная электронная почта | (1.3.6.1.5.5.7.3.4) |
| | Пользователь Центра Регистрации | (1.2.643.2.2.34.6) |

Настоящим я, _____
(фамилия, имя, отчество)

Соглашаюсь с обработкой своих персональных данных Удостоверяющим центром «ЦСК» и признаю, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых я являюсь, относятся к общедоступным персональным данным.

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

Приложение №3
к Регламенту Удостоверяющего центра «ЦСК»
(Форма доверенности Пользователя Удостоверяющего центра)

Доверенность

г. _____ « ____ » _____ 20__ г.

(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

выступать в роли Пользователя Удостоверяющего центра «ЦСК» и осуществлять действия в рамках Регламента Удостоверяющего центра «ЦСК» по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи, установленные для Пользователя Удостоверяющего центра «ЦСК».

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

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

Подпись уполномоченного представителя Фамилия И.О. _____ подтверждаю.

Руководитель организации _____ (_____)
(фамилия, инициалы)

М.П.

Приложение №4
к Регламенту Удостоверяющего центра «ЦСК»
(Форма доверенности на получение ключей электронной подписи
и сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра)

Для юридических лиц

Доверенность

г. _____ « ____ » _____ 20__ г.

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

в лице _____, (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____ (фамилия, имя, отчество)

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

1. Предоставить в Удостоверяющий центр «ЦСК» необходимые документы, определенные Регламентом Удостоверяющего центра «ЦСК» для создания квалифицированного сертификата ключа проверки электронной подписи своего полномочного представителя - Пользователя Удостоверяющего центра «ЦСК»;

2. Получить ключ электронной подписи и сертификат ключа проверки электронной подписи, созданные для пользователя Удостоверяющего центра

_____ (фамилия, имя, отчество Пользователя Удостоверяющего центра)

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

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

Подпись уполномоченного представителя _____ (Фамилия И.О.) _____ (Подпись)

подтверждаю.

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

Руководитель организации _____ (_____)
(фамилия, инициалы)

М.П.

Приложение №4
к Регламенту Удостоверяющего центра «ЦСК»
(Форма доверенности на получение ключей электронной подписи
И сертификата ключа проверки электронной подписи
Пользователя в Удостоверяющем центре)

Для физических лиц

Доверенность*

г. _____ « ____ » _____ 20__ г.

Я, _____
(фамилия, имя, отчество)

_____ (серия и номер паспорта)

_____ кем и когда выдан)

уполномочиваю _____
(фамилия, имя, отчество)

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

1. Предоставить в Удостоверяющий центр «ЦСК» необходимые документы, определенные Регламентом Удостоверяющего центра «ЦСК» для создания на мое имя квалифицированного сертификата ключа проверки электронной подписи;
2. Получить ключ электронной подписи и квалифицированный сертификат ключа проверки электронной подписи, созданные для меня Удостоверяющим центром.

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

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

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

* Настоящая Доверенность должна быть заверена нотариусом

Приложение №5
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на прекращение действия (аннулирование)
сертификата ключа проверки электронной подписи)

Для юридических лиц

Заявление
на прекращение действия (аннулирование) сертификата ключа проверки
электронной подписи Пользователя Удостоверяющего центра «ЦСК»

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

в лице _____, (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

в связи с _____ (причина отзыва сертификата)

Просит прекратить действие (аннулировать) сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра «ЦСК»:

_____ (фамилия, имя, отчество)

содержащий следующие данные:

| | | |
|---|---------------------------------|---------------------|
| Серийный номер сертификата ключа проверки электронной подписи | | |
| Должность | | |
| Фамилия (псевдоним) | | |
| Имя | | |
| Отчество | | |
| Наименование подразделения | | |
| Наименование организации | | |
| Адрес | | |
| ИНН | | |
| ОГРН | | |
| СНИЛС | | |
| Город | | |
| Область | | |
| Страна | RU | |
| Адрес электронной почты | | |
| Области использования ключа | Проверка подлинности клиента | (1.3.6.1.5.5.7.3.2) |
| | Защищенная электронная почта | (1.3.6.1.5.5.7.3.4) |
| | Пользователь Центра Регистрации | (1.2.643.2.2.34.6) |

Пользователь УЦ «ЦСК» _____ (_____) (фамилия, инициалы)

Руководитель организации _____ (_____) (фамилия, инициалы)

М.П.

Приложение №5
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на прекращение действия (аннулирование)
сертификата ключа проверки электронной подписи)

Для физических лиц

Заявление
на прекращение действия (аннулирование) сертификата ключа проверки
электронной подписи Пользователя Удостоверяющего центра «ЦСК»

Я, _____
(фамилия, имя, отчество)

_____ (серия и номер паспорта)

в связи с _____
(причина отзыва сертификата)

Прошу аннулировать (отозвать) выданный на мое имя сертификат ключа подписи,
содержащий следующие данные:

| | | |
|---|---|--|
| Серийный номер сертификата ключа проверки электронной подписи | | |
| Фамилия (псевдоним) | | |
| Имя | | |
| Отчество | | |
| ИНН | | |
| СНИЛС | | |
| Город | | |
| Область | | |
| Страна | | |
| Адрес электронной почты | | |
| Области использования ключа | Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации | (1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6) |

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

« _____ » _____ 20__ г.

Приложение №6
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на приостановление действия сертификата
ключа проверки электронной подписи)

Для юридических лиц

**Заявление
на приостановление действия сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра «ЦСК»**

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

(фамилия, имя, отчество)

действующего на основании _____

Просит приостановить действие сертификат ключа проверки электронной подписи своего
уполномоченного представителя – Пользователя Удостоверяющего центра «ЦСК»:

(фамилия, имя, отчество)

содержащий следующие данные:

| | |
|---|----|
| Серийный номер сертификата ключа проверки электронной подписи | |
| Должность | |
| Фамилия (псевдоним) | |
| Имя | |
| Отчество | |
| Наименование подразделения | |
| Наименование организации | |
| Адрес | |
| ИНН | |
| ОГРН | |
| СНИЛС | |
| Город | |
| Область | |
| Страна | RU |
| Адрес электронной почты | |

Срок приостановления действия сертификата _____ дней
(количество прописью)

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

Руководитель организации _____ (_____)
(фамилия, инициалы)

М.П.

« ____ » _____ 20__ г.

Приложение №6
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на приостановление действия сертификата
ключа проверки электронной подписи)

Для физических лиц

Заявление
на приостановление действия сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра «ЦСК»

Я, _____
(фамилия, имя, отчество)

_____ (серия и номер паспорта)

прошу приостановить действие выданного на мое имя сертификата ключа подписи, содержащего следующие данные:

| | |
|---|--|
| Серийный номер сертификата ключа проверки электронной подписи | |
| Фамилия (псевдоним) | |
| Имя | |
| Отчество | |
| ИНН | |
| СНИЛС | |
| Город | |
| Область | |
| Страна | |
| Адрес электронной почты | |

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

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

«_____» _____ 20__ г.

Приложение №7
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на возобновление действия сертификата
ключа проверки электронной подписи)

Для юридических лиц

Заявление
на возобновление действия сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра «ЦСК»

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

в лице _____, (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие сертификата ключа проверки электронной подписи своего
уполномоченного представителя – Пользователя Удостоверяющего центра «ЦСК»:

_____ (фамилия, имя, отчество)

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

содержащего следующие данные:

| | |
|---|----|
| Серийный номер сертификата ключа проверки электронной подписи | |
| Должность | |
| Фамилия (псевдоним) | |
| Имя | |
| Отчество | |
| Наименование подразделения | |
| Наименование организации | |
| Адрес | |
| ИНН | |
| ОГРН | |
| СНИЛС | |
| Город | |
| Область | |
| Страна | RU |
| Адрес электронной почты | |

Пользователь УЦ «ЦСК» _____ (_____) (фамилия, инициалы)

Руководитель организации _____ (_____) (фамилия, инициалы)

М.П.

« ____ » _____ 20__ г.

Приложение №7
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на возобновление действия сертификата
ключа проверки электронной подписи)

Для физических лиц

Заявление
на возобновление действия сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра «ЦСК»

Я, _____
(фамилия, имя, отчество)

прошу возобновить действие сертификата ключа подписи, содержащего следующие данные:

| | |
|---|--|
| Серийный номер сертификата ключа проверки электронной подписи | |
| Фамилия (псевдоним) | |
| Имя | |
| Отчество | |
| ИНН | |
| СНИЛС | |
| Город | |
| Область | |
| Страна | |
| Адрес электронной почты | |

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

« ____ » _____ 20__ г.

Приложение №8
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на получение информации о статусе сертификата)

Для юридических лиц

Заявление
на получение информации о статусе сертификата ключа проверки электронной подписи,
созданного Удостоверяющим центром «ЦСК»

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

в лице _____, (должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

Просит предоставить информацию о статусе следующего сертификата ключа подписи:

| | |
|---|--|
| Серийный номер сертификата ключа проверки электронной подписи | |
| Должность | |
| Фамилия (псевдоним) | |
| Имя | |
| Отчество | |
| Наименование подразделения | |
| Наименование организации | |
| Адрес | |
| ИНН | |
| ОГРН | |
| СНИЛС | |
| Город | |
| Область | |
| Страна | |
| Адрес электронной почты | |

Время¹ (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

Руководитель организации _____ (_____) (фамилия, инициалы)

М.П.

«_____» _____ 20__ г.

¹ Время и дата должны быть указаны с учетом часового пояса г. Калининграда (по Калининградскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №8
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на получение информации о статусе сертификата
ключа проверки электронной подписи)

Для физических лиц

Заявление
на получение информации о статусе сертификата ключа проверки электронной подписи,
созданного Удостоверяющим центром «ЦСК»

Я, _____
(фамилия, имя, отчество)

Прошу предоставить информацию о статусе следующего сертификата ключа подписи:

| | |
|---|--|
| Серийный номер сертификата ключа проверки электронной подписи | |
| Фамилия (псевдоним) | |
| Имя | |
| Отчество | |
| ИНН | |
| СНИЛС | |
| Город | |
| Область | |
| Страна | |
| Адрес электронной почты | |

Время¹ (период времени) на момент наступления которого требуется установить статус сертификата: с « _____ » по « _____ ».

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

« _____ » _____ 20__ г.

¹ Время и дата должны быть указаны с учетом часового пояса г. Калининграда (по Калининградскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №9
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на подтверждение подлинности электронной подписи)

Для юридических лиц

Заявление
на подтверждение подлинности электронной подписи в электронном документе

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

в лице _____,
(должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

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

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № _____;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № _____.

3. Время¹ подписания электронной подписью электронного документа:

« _____ : _____ » « _____ / _____ / _____ »;
Час минута день месяц год

Если момент подписания электронного документа не определен, то указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:

« _____ : _____ » « _____ / _____ / _____ ».
Час минута день месяц год

Руководитель организации _____ (_____)
(фамилия, инициалы)

М.П.

« _____ » _____ 20__ г.

¹ Время и дата должны быть указаны с учетом часового пояса г. Калининграда (по Калининградскому времени). Если время и дата не указаны, то подтверждение подлинности электронной подписи устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №9
к Регламенту Удостоверяющего центра «ЦСК»
(Форма заявления на подтверждение подлинности электронной подписи)

Для физических лиц

Заявление
на подтверждение подлинности электронной подписи в электронном документе

Я, _____
(фамилия, имя, отчество)

прошу подтвердить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № _____;

2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № _____.

3. Время¹ подписания электронной подписью электронного документа:

« _____ : _____ » « _____ / _____ / _____ »;
Час минута день месяц год

Если момент подписания электронного документа не определен, то указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:

« _____ : _____ » « _____ / _____ / _____ ».
Час минута день месяц год

Пользователь УЦ «ЦСК» _____ (_____)
(фамилия, инициалы)

« _____ » _____ 20 ____ г.

¹ Время и дата должны быть указаны с учетом часового пояса г. Калининграда (по Калининградскому времени). Если время и дата не указаны, то подтверждение подлинности электронной подписи устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №10
к Регламенту Удостоверяющего центра «ЦСК»
(Форма сертификата (копии сертификата) ключа
проверки электронной подписи на бумажном носителе)

ООО «Цифровые системы контроля»
Удостоверяющий центр «ЦСК»
Сертификат ключа проверки электронной подписи

Сведения о сертификате:**Кому выдан:**

Фамилия Имя Отчество

Кем выдан:

УЦ ЦСК

Действителен с 15 января 2013 г. 12:03:00 UTC по 15 января 2014 г. 12:12:00 UTC

Версия: 3 (0x2)**Серийный номер:** 6109 5AF2 0001 0000 0259**Издатель сертификата:** CN = УЦ ЦСК, OU = Удостоверяющий центр, O = ООО «ЦСК», L = Калининград, S = 39 Калининградская область, C = RU, E = uc@dsyst.com, ИHN = 003906143236, ОГРН = 1053903302584**Срок действия:**

Действителен с: 15 января 2013 г. 12:03:00 UTC

Действителен по: 15 января 2014 г. 12:12:00 UTC

Владелец сертификата: T = Должность, STREET = Адрес, CN = Фамилия Имя Отчество, O = Организация, L = Калининград, S = 39 Калининградская область, C = RU, E = электронная почта, ИHN = 00XXXXXXXXXX, ОГРН = XXXXXXXXXXXXX, СНИЛС = XXXXXXXXXXXX**Ключ проверки электронной подписи:**

Алгоритм ключа проверки электронной подписи:

Название: ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.19

Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01

Значение: 0481 80A4 5A5B 0041 B273 F51E B062 322E CE6B 0480 5702 3FFF 5312 8FBA 1163 7381 5FED 445C 7DF9 F764 7822 99AA 3C3D 1E23

FE69 B714 7062 36ED CB4A A834 7D5A 3525 BAC2 D80C 53DC 781B 4180 7CD3 ADD1 6D0E 00C9 9CA0 432F 595F 9CD3 12BE 69E6 A4D6 6133 227C

DE1A 80F4 DOF1 8337 843E CAD1 561F 793B CB05 EEBV EBD4 C23F E5EA ECD9 E6B5 A9

Расширения сертификата X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных(F0)

2. Расширение 2.5.29.37

Название: Улучшенный ключ

Значение: Защищенная электронная почта(1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)

3. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: 56BD CA83 3029 0673 CA83 3381 16D4 AF10 C3D6 9A75

4. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение: Идентификатор ключа=50AA 3E1E 4186 F8DC 3585 6E11 2C11 D9E3 0A91 7AD7 Поставщик сертификата: Адрес каталога: CN = УЦ ЦСК, OU = Удостоверяющий центр, O = «ООО «ЦСК»», L = Калининград, S = 39 Калининградская область, C = RU, E = uc@dsyst.com, ИHN = 003906143236, ОГРН = 1053903302584 Серийный номер сертификата=55 87 17 9c 56 7a bc 77 3c f1 72 4f 40 5d 7d 5b

5. Расширение 2.5.29.31

Название: Точки распространения списков отзыва (CRL)

Значение: [1]Точка распространения списка отзыва (CRL) Имя точки распространения: Полное имя:

URL=http://www.dsyst.com/index/cert_63.crl

6. Расширение 1.3.6.1.5.5.7.1.1

Название: Доступ к информации о центрах сертификации

Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния сертификата через сеть

(1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://www.dsyst.com/ocsp63/ocsp.srf [2]Доступ к сведениям центра сертификации Метод

доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://www.dsyst.com/index/uc_csk_63.cer

7. Расширение 2.5.29.16

Название: Период использования закрытого ключа

Значение: Действителен с 15 января 2013 г. 12:03:00 Действителен по 15 января 2014 г. 12:12:00

8. Расширение 2.5.29.32

Название: Политики сертификата

Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1

9. Расширение 1.2.643.100.111

Название: Средство электронной подписи владельца

Значение: Средство электронной подписи: «КриптоПро CSP» (версия 3.6)

10. Расширение 1.2.643.100.112

Название: Средства электронной подписи и УЦ издателя

Значение: Средство электронной подписи: «КриптоПро CSP» (версия 3.6) Заключение на средство ЭП: СФ/111-1858 от 17 июня 2012 г. Средство

УЦ: «Удостоверяющий центр «КриптоПро УЦ» версии 1.5 Заключение на средство УЦ: СФ/128-1822 от 01 июня 2012 г.

Подпись Удостоверяющего центра:

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-2001

Идентификатор: 1.2.643.2.2.3

Значение: 826C DDFB 331C 58C5 FD3D 9233 4A1D 2D7A B973 387C 8E8A DD3D 6FCE 0573 508A 3DC4 B29F 5961 FB6C D1EB 1B40 37C7 8473 5B0F FECA 5E38 EA0C 3890 C77A C97E BD18 873A

Администратор Удостоверяющего центра «ЦСК»

_____ / _____

« ____ » _____ 20__ г.

М.П.

Подпись владельца сертификата: _____ / _____

" ____ " _____ 20__ г.