УТВЕРЖДАЮ

Директор государственного бюджетного учреждения Волгоградской области "Центр информационных технологий Волгоградской области"

_____А.В. Несытов

"17" февраля 2021

РЕГЛАМЕНТ

ОКАЗАНИЯ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

государственного бюджетного учреждения Волгоградской области " Центр информационных технологий Волгоградской области"

Редакция 2.9.

Волгоград, 2021

Содержание

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Владелец сертификата ключа подписи (Пользователь УЦ) - лицо, которому Удостоверяющим центром в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" выдан сертификат ключа проверки электронной подписи.

Единая система идентификации и аутентификации – информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах.

Запрос на издание сертификата (Запрос) – электронный документ, подписанный ключом электронной подписи, содержащий соответствующий ему ключ проверки электронной подписи, сведения о Заявителе, а также другие сведения, предназначенные для включения в сертификат ключа подписи, формируемый Удостоверяющим центром на основании Запроса. Формат запроса определен PKCS#10.

Заявитель - лицо, обратившееся в Удостоверяющий центр за получением сертификата ключа электронной подписи и/или другими услугами Удостоверяющего центра.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Квалифицированный сертификат ключа подписи (квалифицированный сертификат, сертификат ключа подписи) - электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром и подтверждающие принадлежность ключа подписи Пользователю УЦ.

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

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи Удостоверяющего центра – ключ электронной подписи, владельцем которого является Удостоверяющий центр, и который используется Уполномоченным лицом Удостоверяющего центра для подписания электронной подписью выпускаемых сертификатов ключей подписей.

Ключевой документ – ключевой носитель, содержащий ключ электронной подписи, а при необходимости, сертификат ключа подписи;

Ключевой носитель – носитель информации, предназначенный, в соответствии с правилами пользования средствами электронной подписи, для размещения на нем ключей электронной подписи;

Компрометация ключа электронной подписи - утрата доверия к тому, что в отношении ключа электронной подписи соблюдена конфиденциальность. Ключ электронной подписи считается скомпрометированным, если:

1) явным образом нарушена конфиденциальность ключа электронной подписи (утрачен ключевой документ, выявлено несанкционированное использование ключа электронной подписи др.);

2) существуют основания полагать, что конфиденциальность ключа электронной подписи нарушена (уволен работник, имевший доступ к ключевому документу, произошла утрата ключевого документа с последующим обнаружением, нарушена целостность печатей на сейфах (шкафах, ящиках, хранилищах, контейнерах и т.п.), используемых для хранения ключевых документов и др.);

Ответственное лицо - работник юридического лица, наделенный полномочиями осуществлять взаимодействие с Удостоверяющим центром с целью осуществления организации выдачи и аннулирования сертификатов ключей проверки электронных подписей соответствующего юридического лица.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 8:30 по 17:30 (местное время) каждого дня недели за исключением выходных и праздничных дней.

Реестр квалифицированных сертификатов (Реестр сертификатов) - формируемый Удостоверяющим центром в соответствии с Порядком формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Министерства связи и массовых коммуникаций Российской Федерации от 5 октября 2011 г. N 250 (далее – Порядок ведения реестра) реестр выданных и аннулированных квалифицированных сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных сертификатах ключей проверки электронных подписей, информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования, а также иную информацию предусмотренную Порядком ведения реестра;

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

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации следующих функций:

–создание электронной подписи;

–проверка электронной подписи;

–создание ключа электронной подписи и ключа подписи.

Удостоверяющий центр – Государственное бюджетное учреждение Волгоградской области "Центр информационных технологий Волгоградской области", признанное уполномоченным федеральным органом в сфере использования электронной подписи соответствующим требованиям Федерального закона от 06 апреля 2011 г. № 63-ФЗ "Об электронной подписи" и осуществляющее функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронной подписи, а также иные функции, предусмотренные Федеральным законом "Об электронной подписи".

Уполномоченное лицо Удостоверяющего центра – работник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по заверению сертификатов ключей подписей и списков аннулированных сертификатов.

Уполномоченное лицо юридического лица (Пользователь сертификата) - физического лицо, уполномоченное юридическим лицом, действовать от имени юридического лица при осуществлении обмена информацией в электронной форме с применением электронной подписи, и указываемое наряду с указанием юридического лица в качестве владельца сертификата ключа подписи (в случае внесения в сертификат ключа подписи сведений о таком физическом лице)[1].

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

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

– присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией;

– используется для определения лица, подписывающего информацию;

– получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

– позволяет определить лицо, подписавшее электронный документ;

[1] Допускается не указывать в качестве владельца сертификата ключа подписи физическое лицо, действующее от имени юридического лица, в сертификате ключа подписи, используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами.

– позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

– ключ проверки электронной подписи указан в сертификате ключа подписи;

– для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06 апреля 2011 г. N63-ФЗ "Об электронной подписи".

Электронная подпись - информация в электронной форме, которая соответствует следующим признакам:

Cryptographic Message Syntax (CMS) – стандарт, определяющий формат и синтаксис криптографических сообщений, реализующий RFC 3852 "Cryptographic Message Syntax".

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

Certification Request Syntax Specification (PKCS #10) – стандарт, определяющий формат и синтаксис запросов на создание сертификатов, реализующий RFC 2986 "PKCS #10: Certification Request Syntax Specification. Version 1.7".

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

Ответственное лицо - работник юридического лица, наделенный полномочиями осуществлять взаимодействие с Удостоверяющим центром с целью осуществления организации выдачи и аннулирования сертификатов ключей проверки электронных подписей соответствующего юридического лица.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Сведения об Удостоверяющем центре

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

Удостоверяющий центр осуществляет свою деятельность на основании следующих лицензий:

Лицензия Управления Федеральной службы безопасности Российской Федерации по Волгоградской области N 162-Н от 27 августа 2020 г. на осуществление деятельности:

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

Информация по аккредитации представлена на официальном сайте Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации: https://digital.gov.ru/ru/activity/govservices/2/.

2.2. Контактная информация

Государственное бюджетное учреждение Волгоградской области "Центр информационных технологий Волгоградской области" (ГБУ ВО "ЦИТ ВО"), именуемое в дальнейшем "Удостоверяющий центр" (сокращенно – УЦ), зарегистрировано на территории Российской Федерации в городе Волгограде.

Юридический адрес: 400012 г., Волгоград, ул. Витимская, 15 А, офис 405

Фактический адрес: 400012 г., Волгоград, ул. Витимская, 15 А, офис 405

Контактная информация:
Техническая поддержка: (8442) 35-22-45
Служба регистрации Удостоверяющего центра: (8442) 35-22-66
E-mail: ca@volganet.ru
Сайт: http://citvo.ru/struct/ca/ecp/

Адреса (точки распространения) списков аннулированных сертификатов и сертификата ключа подписи Удостоверяющего центра в информационно-телекоммуникационной сети "Интернет" указываются в соответствующих полях сертификатов ключей подписей Пользователей УЦ.

2.3. Регламент оказания услуг Удостоверяющего центра

2.3.1. Идентификация Регламента

Наименование документа: "Регламент оказания услуг Удостоверяющего центра Государственного бюджетного учреждения Волгоградской области "Центр информационных технологий Волгоградской области".

2.3.2. Статус Регламента

Регламент оказания услуг Удостоверяющего центра, именуемый в дальнейшем "Регламент", разработан в соответствии с действующим законодательством Российской Федерации, регулирующим отношения в области использования электронных подписей.

Настоящий Регламент является договором присоединения на основании статьи 428 Гражданского кодекса Российской Федерации.

Настоящий Регламент определяет механизмы и условия предоставления и использования услуг Удостоверяющего центра, включая обязанности Заявителей, Пользователей УЦ и работников Удостоверяющего центра, основные организационно-технические мероприятия, необходимые для безопасной работы Удостоверяющего центра.

2.3.3. Распространение Регламента

Настоящий Регламент распространяется:

1) в форме электронного документа на сайте Удостоверяющего центра http://citvo.ru/struct/ca/ecp/RegCA.pdf или по электронной почте по запросу заинтересованного лица;

2) в форме документа на бумажном носителе - по адресу Удостоверяющего центра.

2.3.4. Присоединение к Регламенту

Присоединение к настоящему Регламенту осуществляется путем подписания и представления заинтересованным лицом в Удостоверяющий центр заявления о присоединении к Регламенту (Приложение N 1 – для физических лиц, N 2 – для юридических лиц).

Срок присоединения к Регламенту устанавливается на срок оказания услуг или срок действия результатов оказания услуг.

С момента регистрации заявления о присоединении к Регламенту в Удостоверяющем центре лицо, подавшее заявление, считается присоединившимся к Регламенту и является стороной Регламента.

Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации заявления о присоединении к Регламенту с обоснованием причины отказа.

Факт присоединения к Регламенту является полным принятием 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.

2.3.5. Область применения Регламента

Настоящий Регламент предназначен служить соглашением, налагающим обязательства всем вовлеченным сторонам, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг Удостоверяющего центра.

2.3.6. Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент (внесение изменений и дополнений в Регламент) утверждается руководителем Удостоверяющего центра.

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

Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений (дополнений) на сайте Удостоверяющего центра.

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 с момента размещения указанных изменений и дополнений в Регламенте на сайте Удостоверяющего центра.

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

Любые изменения и дополнения в Регламент 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 присоединения к Регламенту.

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

2.3.7. Прекращение действия Регламента

Действие настоящего Регламента, может быть, прекращено по инициативе одной из сторон в следующих случаях:

- по собственному желанию одной из сторон;
- нарушения одной из сторон условий настоящего Регламента.

В случае прекращения действия Регламента инициативная сторона письменно уведомляет другую сторону о своих намерениях за десять календарных дней до даты расторжения Регламента. Регламент считается расторгнутым после выполнения сторонами своих обязательств и проведения взаиморасчетов согласно условиям Регламента.

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).

2.3.8. Стоимость услуг Удостоверяющего центра

Стоимость, сроки и порядок расчетов за оказанные услуги Удостоверяющего центра регулируются договором между Сторонами, согласно прейскуранту на платные услуги размещенного на официальном сайте Удостоверяющего центра по адресу citvo.ru .

Доступ к Реестру сертификатов Удостоверяющего центра предоставляется на безвозмездной основе.

В случае выполнения внеплановой смены ключей уполномоченного лица Удостоверяющего центра в соответствии с процедурой, определенной Регламентом, Удостоверяющий центр осуществляет перевыпуск сертификатов ключей подписей безвозмездно.

Удостоверяющий центр выполняет аннулирование сертификатов ключей подписей безвозмездно.

2.4. Перечень функций (оказываемых услуг), реализуемых Удостоверяющим центром

В перечень реализуемых Удостоверяющим Центром функций (оказываемых услуг) в соответствии с настоящим Регламентом, входят:

- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата;
- осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- осуществляет иную связанную с использованием электронной подписи деятельность.

2.5. Права и обязанности Удостоверяющего центра

2.5.1. Удостоверяющий центр обязан:

1) Информировать в письменной форме Заявителей об условиях и о порядке использования ЭП и средств электронной подписи, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

2) Обеспечивать актуальность информации, содержащейся в Реестре

сертификатов, ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3) Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к Реестру сертификатов информацию, содержащуюся в Реестре сертификатов, в том числе информацию об аннулировании Сертификата.

4) Обеспечивать конфиденциальность созданных УЦ ключей ЭП.

5) Отказать заявителю в создании Сертификата в случае, если не было подтверждено то, что Заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному заявителем для получения Сертификата.

6) Отказать Заявителю в создании Сертификата в случае отрицательного результата проверки в Реестре сертификатов уникальности ключа проверки ЭП, указанного Заявителем для получения Сертификата.

7) При прекращении деятельности УЦ:

- сообщить в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

- передать в уполномоченный федеральный орган в установленном порядке Реестр выданных УЦ квалифицированных Сертификатов;

- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном УЦ.

8) При прекращении деятельности УЦ с переходом его функций другим лицам:

- уведомить в письменной форме Владельцев сертификатов Ключей проверки ЭП, которые выданы УЦ и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций;

- передать информацию, внесенную в Реестр сертификатов, лицу, к которому перешли функции УЦ.

9) В случае прекращения деятельности УЦ без перехода его функций другим лицам:

- уведомить в письменной форме Владельцев сертификатов, выданные УЦ и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности УЦ (в указанном случае после прекращения деятельности УЦ информация, внесенная в Реестр сертификатов, будет уничтожена).

10) Вносить информацию о Сертификатах в Реестр сертификатов не позднее указанной в нем даты начала действия такого Сертификата.

11) Вносить информацию о прекращении действия Сертификата в Реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона № 63-ФЗ, или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие Сертификата прекращается с момента внесения записи об этом в Реестр сертификатов.

12) Уведомить Владельца сертификата об аннулировании его Сертификата путем направления электронного документа по электронной почте, указанной в заявлении на изготовление Сертификата до внесения в Реестр сертификатов информации об аннулировании.

13) Хранить информацию, указанную в части 1 статьи 15 Федерального закона № 63-ФЗ, в течение срока деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, в форме, позволяющей проверить ее целостность и достоверность, а именно:

- реквизиты основного документа, удостоверяющего личность Владельца сертификата - физического лица;

- сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени Заявителя - юридического лица, обращаться за получением Сертификата;

- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия Владельца сертификата действовать по поручению третьих лиц, если информация о таких полномочиях Владельца сертификата включена в квалифицированный Сертификат.

14) Для подписания от своего имени квалифицированных Сертификатов и списков аннулированных Сертификатов использовать квалифицированную электронную подпись, основанную на квалифицированном Сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган.

15) Не использовать квалифицированную электронную подпись, основанную на квалифицированном Сертификате, выданном головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания Сертификатов, не являющихся квалифицированными Сертификатами.

16) Обеспечить любому лицу безвозмездный доступ с использованием информационно - телекоммуникационных сетей, в том числе сети "Интернет", к Реестру сертификатов УЦ в любое время в течение срока деятельности УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

17) Соблюдать требования, на соответствие которым УЦ аккредитован, в течение всего срока аккредитации. В случае возникновения обстоятельств, делающих невозможным соблюдение указанных требований, УЦ немедленно уведомляет об этом в письменной форме уполномоченный федеральный орган.

18) Выполнять порядок реализации функций УЦ и исполнять обязанности УЦ, установленные настоящим Регламентом.

19) Осуществить присоединение информационной системы, обеспечивающей реализацию функций аккредитованного УЦ к информационно-технологической и коммуникационной инфраструктуре в порядке, установленном в соответствии с частью 4 статьи 19 Федерального закона от 27.07.2010 № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг".

20) При выдаче Сертификата идентифицировать Заявителя – физического лица, обратившегося за получением Сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации". отказать в проведении идентификации Заявителю, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы *отказывается* от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации.

21) получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата;

при выдаче Сертификата идентифицировать заявителя - физическое лицо, выступающего от имени юридического лица, подтверждения правомочия обращаться за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации,

содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

22) Ознакомить Заявителя под расписку с информацией, содержащейся в Сертификате при выдаче Сертификата.

23) Одновременно с выдачей Сертификата выдать Владельцу сертификата руководство по обеспечению безопасности использования квалифицированной ЭП и средств ЭП - Правила использования СКЗИ и ЭП (Приложению №1 к настоящему Регламенту).

24) Направлять в единую систему идентификации и аутентификации сведения о лице, получившем Сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им Сертификате (уникальный номер Сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного УЦ).

25) По желанию лица, которому выдан Сертификат безвозмездно осуществлять регистрацию лица в единой системе идентификации и аутентификации при выдаче Сертификата.

26) Вносить в Сертификат только достоверную информацию, подтвержденную соответствующими документами.

27) Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Волгограда и синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

28) Уведомлять Пользователей УЦ о фактах, которые стали известны Удостоверяющему центру, и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи.

2.5.2. Удостоверяющий центр вправе:

1) Наделять третьих лиц полномочиями по вручению Сертификата от имени УЦ.

2) Выдавать Сертификаты, как в форме электронных документов, так и в форме документов на бумажном носителе.

3) Не представлять документ, подтверждающий соответствие имеющихся средств электронной подписи и средств удостоверяющего центра требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, если такой документ или содержащиеся в нем сведения находятся в распоряжении федерального органа исполнительной власти в области обеспечения безопасности.

4) Отказать в изготовлении Сертификата Заявителю в случае непредставления документов, предоставления документов не в полном объеме или предоставления документов, подлинность которых вызывает сомнение.

5) Отказать в изготовлении Сертификата Заявителю в случае, если использованное Заявителем для формирования запроса на Сертификат СКЗИ не поддерживается УЦ.

6) Отказать в изготовлении Сертификата Заявителю в случае невыполнения Заявителем обязанностей, установленных Федеральным законом № 63-ФЗ, принимаемыми в соответствии с ним нормативными правовыми актами, а также Регламентом УЦ.

7) Отказать в изготовлении Сертификата, если предоставленные Заявителем сведения не прошли проверку в соответствии с п.2.2, 2.3 ст.18 Федерального закона № 63- ФЗ, в том числе

8) Отказать в изготовлении Сертификата Заявителю при расхождении данных, предоставленных Заявителем с данными, указанными в ЕГРЮЛ или ЕГРИП.

9) Аннулировать Сертификат, в случае установленного факта компрометации соответствующего Ключа ЭП, с уведомлением Владельца аннулированного Сертификата по электронной почте, указанной при заполнении заявления на Сертификат.

10) Проверять достоверность документов и сведений, предоставленных Заявителем, с использованием инфраструктуры, запрашивать и получать из государственных информационных ресурсов:

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

- выписку из единого государственного реестра индивидуальных предпринимателей в отношении Заявителя – индивидуального предпринимателя;

- выписку из Единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

2.5.3. Владелец (Пользователь УЦ) обязан:

1) Обеспечить конфиденциальность ключа ЭП. Уведомить УЦ о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении. Не использовать ключ ЭП и немедленно обратиться в аккредитованный УЦ, выдавший Сертификат, для прекращения действия этого Сертификата при наличии оснований полагать, что конфиденциальность ключа ЭП нарушена.

2) Использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены).

3) Извещать УЦ о внесении изменений в документы, на основании которых УЦ были выпущены сертификаты ключей, в течение не более чем одного рабочего дня со дня внесения изменений и по требованию УЦ предоставить их течение 5 (пяти) рабочих дней с момента регистрации изменений;

4) При подаче заявления на Сертификат указать действующий электронный почтовый адрес Владельца сертификата для получения извещений, уведомлений от УЦ, связанных с применением Сертификата, его аннулированием.

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

6) Применять для формирования ЭП только действующий личный закрытый ключ.

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

8) Использовать ЭП в соответствии с ограничениями, содержащимися в Сертификате (если такие ограничения установлены).

9) Немедленно обратиться в УЦ с заявлением на аннулирование действия Сертификата в случае утери, кражи, а также в случае если Владельцу сертификата стало известно, что ключ ЭП используется или использовался ранее другими лицами.

10) Не использовать личный закрытый ключ, связанный с Сертификатом, заявление на аннулирование которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование Сертификата по момент времени официального уведомления об аннулировании Сертификата.

11) Не использовать личный закрытый ключ, связанный с Сертификатом, который аннулирован.

12) Ознакомиться с условиями о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки (приложение N 10 к настоящему Регламенту);

13) Для проведения плановой замены в связи истечением срока действия сертификатов ключей подписей обращаться в Удостоверяющий центр не ранее чем за 30 (тридцать) и не позднее, чем за 5 (пять) дней до истечения их сроков действия.

14) Владелец (Пользователь УЦ) – юридическое лицо также обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и принятыми в

соответствии с ним нормативными правовыми актами при передаче персональных данных уполномоченных лиц в Удостоверяющий центр в целях изготовления сертификатов ключей подписей.

2.5.4. Владелец (Пользователь УЦ) имеет право:

1) Владелец сертификата, выданного в форме электронного документа, вправе получить также копию Сертификата на бумажном носителе, заверенную УЦ.

2) Обратиться в УЦ с заявлением на изготовление Сертификата.

3) Обратиться в УЦ с заявлением на аннулирование Сертификата, владельцем которого он является, в течение срока действия соответствующего Сертификата.

4) Обратиться в УЦ за получением информации о статусе Сертификата и их действительности на определенный момент времени.

5) Обратиться в УЦ за подтверждением действительности ЭП в электронном документе, сформированной с использованием Сертификата, изданного УЦ.

3. РАЗРЕШЕНИЕ СПОРОВ

Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Пользователь УЦ.

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

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

Сторона, получившая от другой Стороны претензию, обязана в течение 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.

При разрешении в претензионном порядке споров, связанных с использованием электронной подписи, в обязательном порядке производится экспертиза, для осуществления которой привлекается Удостоверяющий центр, изготовивший сертификат ключа подписи, с использованием которого сформирована электронная подпись, в отношении которой возник спор.

Экспертиза проводится в порядке, установленном Удостоверяющим центром, или соответствующим соглашением сторон.

Спорные вопросы между сторонами, неурегулированные в претензионном порядке, решаются в судебном порядке в соответствии с действующим законодательством.

4. ОТВЕТСТВЕННОСТЬ СТОРОН

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.

Ни одна из сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая сторона.

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 представленных Пользователем УЦ документах.

5. ПРОЦЕДУРЫ И МЕХАНИЗМЫ

5.1. Изготовление сертификата ключа подписи

Удостоверяющий центр осуществляет изготовление сертификата ключа подписи только в том случае, если Заявитель присоединился к Регламенту в соответствии с пунктом 2.3.4. Регламента.

Прием документов для изготовления сертификатов ключей подписей осуществляется Удостоверяющим центром по предварительной записи. Запись на прием осуществляется по телефону, номер которого публикуется на сайте Удостоверяющего центра http://citvo.ru.

Срок оказания услуги по изготовлению сертификата ключа подписи осуществляется Удостоверяющим центром, в течение 7 (семи) рабочих дней, с момента предоставления в Удостоверяющий центр полного комплекта документов, необходимых для изготовления сертификата ключа подписи, а также, при необходимости, ключевого носителя и Запроса.

Удостоверяющий центр с учетом требований владельцев информационных систем и/или организаторов сетей доверия удостоверяющих центров может устанавливать дополнительные требования и определять другой порядок изготовления сертификата ключа подписи, оформляемый в виде дополнения к Регламенту.

Заявители – юридические лица при обращении в Удостоверяющий центр за изготовлением ключей электронной подписи и (или) сертификатов ключей подписей предоставляют заявку на оказание услуг. Форма заявки приведена в Приложении 3 к настоящему Регламенту.

Ключи электронной цифровой подписи и сертификат ключа подписи создаются Удостоверяющим центром на основании заявлений установленной формы (согласно Приложению 4 к настоящему Регламенту – для юридических лиц, Приложению 5 – для физических лиц).

Изготовление ключей электронных подписей и ключей проверки электронных подписей может осуществляться заявителем самостоятельно. В этом случае Удостоверяющий центр осуществляет изготовление сертификата ключа подписи с использованием Запроса, предоставляемого Заявителем.

Подача заявлений и получение сертификатов ключей подписей для Заявителей – юридических лиц осуществляется Ответственным лицом, действующим на основании доверенности или иного документа, подтверждающей его полномочия осуществлять взаимодействие с Удостоверяющим центром (примерная форма доверенности приведена в Приложении 6 к настоящему Регламенту).

Подача заявлений и получение сертификатов ключей подписей для Заявителей – физических лиц осуществляется Заявителем лично или его представителем.

При подаче заявления Заявителем также представляются следующие документы, подтверждающие достоверность информации, предназначенной для включения в сертификат ключа подписи, или их надлежащим образом заверенные копии:

1) основной документ, удостоверяющий личность;

2) страховой номер индивидуального лицевого счета заявителя - физического лица;

3) идентификационный номер налогоплательщика заявителя - физического лица;

4) основной государственный регистрационный номер заявителя - юридического лица;

5) основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя - индивидуального предпринимателя;

6) номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации;

7) документ, подтверждающий право заявителя действовать от имени юридического лица без доверенности либо подтверждающий право заявителя действовать от имени государственного органа или органа местного самоуправления.

При поступлении заявления работник Удостоверяющего центра:

1) устанавливает личность лица (Ответственного лица, Заявителя - физического лица (или

его представителя)), обратившегося за получением сертификата по основному документу, удостоверяющему его личность;

2) осуществляет проверку сведений, указанных в заявлении, на предмет соответствия данным, содержащимся в документах, их подтверждающих;

3) в случае изготовления сертификата ключа подписи на основании Запроса, сравнивает содержимое запроса с данными, указанными в заявлении на изготовление сертификата ключа подписи;

4) на заявлении (для юридических лиц – на заявке), в зависимости от результата проверки, ставит отметку о принятии или отказе (с указанием причины) принятия к обработке, проставляет текущую дату, и заверяет своей подписью;

5) при положительных результатах проверки (сведений, Запроса) осуществляет:

– при формировании ключей электронной подписи Удостоверяющим центром - изготовление и запись на ключевой носитель, предоставляемый Удостоверяющим центром или Заявителем, ключей электронной подписи и сертификата ключа подписи в форме электронного документа;

– при самостоятельном формировании ключей электронной подписи Заявителем - изготовление сертификата ключа подписи на основании Запроса.

6) при необходимости изготавливает копию сертификата ключа подписи в форме документа на бумажном носителе, которая заверяется работником Удостоверяющего центра и печатью Удостоверяющего центра;

7) знакомит Заявителя под роспись с информацией, содержащейся в сертификате ключа подписи.

По окончании процедуры изготовления сертификата ключа подписи Заявителю выдаются:

1) ключи электронной подписи, записанные на ключевой носитель (в случае их изготовления Удостоверяющим центром);

2) сертификат ключа подписи в виде электронного документа;

3) копия сертификата ключа подписи в виде документа на бумажном носителе, заверенная подписью работника и печатью Удостоверяющего центра (по запросу Заявителя);

4) сертификат ключа подписи Удостоверяющего центра в виде электронного документа;

5) руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи.

5.2. Прекращение действия сертификата ключа подписи

Сертификат ключа подписи прекращает свое действие:

1) в связи с истечением установленного срока его действия;

2) на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

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

4) в случае компрометации ключа электронной подписи Удостоверяющего центра, с использованием которого был издан сертификат ключа подписи;

5) в случае прекращения действия настоящего Регламента в отношении Пользователя УЦ;

6) в случае, если не подтверждено, что Пользователь УЦ владеет ключом электронной подписи, соответствующим ключу подписи, указанному в сертификате ключа подписи;

7) в случае, если установлено, что содержащийся в сертификате ключа подписи ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа подписи;

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

9) в иных случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами.

Информация о прекращении действия сертификата ключа подписи вносится

Удостоверяющим центром в реестр сертификатов после уведомления Пользователя УЦ об аннулировании его сертификата ключа подписи.

Информация о прекращении действия сертификата ключа подписи вносится удостоверяющим центром в реестр сертификатов в течение двенадцати часов с момента наступления вышеуказанных обстоятельств или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

Действие сертификата ключа подписи прекращается с момента внесения записи об этом в реестр сертификатов.

Не позднее 1 (одного) часа с момента прекращения действия сертификата ключа подписи Удостоверяющий центр формирует и осуществляет публикацию на сайте Удостоверяющего центра списка аннулированных сертификатов, содержащий сведения об аннулированном сертификате ключа подписи (в т.ч. причину и время аннулирования).

В случае аннулирования сертификата ключа подписи по истечении срока его действия информация об аннулированном сертификате ключа подписи в список аннулированных сертификатов не заносится.

В случае компрометации ключа электронной подписи Удостоверяющего центра временем аннулирования сертификата ключа подписи признается время компрометации ключа электронной подписи Удостоверяющего центра. В случае компрометации ключа электронной подписи Удостоверяющего центра информация об аннулировании сертификата ключа подписи владельцев сертификатов в список аннулированных сертификатов не заносится.

Информация о размещении (точках распространения) списков аннулированных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей подписей.

Для получения нового сертификата ключа подписи выполняются действия в соответствии с п. 5.1 настоящего Регламента.

5.2.1. Порядок аннулирования сертификата ключа подписи по заявлению, подаваемому в виде документа на бумажном носителе

Подача заявления на аннулирование сертификата ключа подписи осуществляется Ответственным лицом Пользователя УЦ - юридическим лица при его личном прибытии в Удостоверяющий центр. Форма заявления приведена в Приложении 8 к настоящему Регламенту.

Пользователь УЦ – физическое лицо подает заявление на аннулирование сертификата ключа подписи по форме, определенной Приложением 9 к настоящему Регламенту лично или через представителя, действующим на основании доверенности по форме, определенной Приложением 7 к настоящему Регламенту.

Заявление предоставляется в Удостоверяющий центр в двух экземплярах.

Прием заявлений и их рассмотрение осуществляется только в течение рабочего дня Удостоверяющего центра.

При поступлении заявления работник Удостоверяющего центра:

1) осуществляет идентификацию лица, предоставившего заявление, по основному документу, удостоверяющему его личность;

2) проверяет сведения, указанные в заявлении;

3) на заявлении, в зависимости от результата проверки, ставит отметку о принятии или отказе (с указанием причины) принятия заявления к обработке, проставляет регистрационный номер, текущие дату и время, заверяет своей подписью и возвращает экземпляр Пользователю УЦ;

4) в случае принятия заявления к обработке обеспечивает аннулирование сертификата ключа подписи.

Отметка работника Удостоверяющего центра о принятии заявления к обработке является уведомлением Пользователя УЦ об аннулировании сертификата ключа подписи.

5.2.2. Порядок аннулирования сертификата ключа подписи по заявлению, подаваемому в форме электронного документа

Заявление на аннулирование сертификата ключа подписи в форме электронного документа направляется в Удостоверяющий центр в виде электронного документа, соответствующего стандарту криптографических сообщений CMS, с электронной подписью Пользователя УЦ. Формирование электронной подписи осуществляется с использованием выданного Удостоверяющим центром, действующего и не аннулируемого по данному заявлению сертификата ключа подписи. Для Пользователя УЦ – юридического лица используется сертификат ключа подписи, выданный на имя руководителя организации, или Уполномоченного лица, действующего на основании доверенности. Такая доверенность должна быть предоставлена в Удостоверяющий центр до момента подачи заявления на аннулирование сертификата ключа подписи в форме электронного документа.

Текст запроса на аннулирование сертификата ключа подписи должен содержать следующие данные:

1) серийный номер аннулируемого сертификата ключа подписи;

2) причину аннулирования из следующего перечня значений ("Выход из строя ключевого носителя", "Компрометация ключа", "Прекращение полномочий уполномоченного лица", "Изменение идентификационных данных/реквизитов владельца", "Другое");

3) дополнительные сведения, поясняющие причину отзыва.

Прием заявлений на аннулирование сертификата ключа подписи в форме электронного документа осуществляется круглосуточно по электронной почте на адрес request@citvo.ru, их рассмотрение осуществляется только в течение рабочего дня Удостоверяющего центра.

При поступлении заявления работник Удостоверяющего центра:

1) осуществляет проверку электронной подписи заявления и содержащихся в нем сведений;

2) формирует в зависимости от результата проверки, уведомление об аннулировании сертификата ключа подписи или об отказе (с указанием причины) принятия заявления к обработке в виде электронного документа;

3) подписывает сформированное уведомление электронной подписью и направляет по электронной почте владельцу сертификата;

4) в случае принятия заявления к обработке обеспечивает аннулирование сертификата ключа подписи.

5.3. Предоставление информации о статусе сертификата ключа подписи

Получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром, осуществляется на основании заявления в простой письменной форме о предоставлении информации о статусе сертификата ключа подписи, направляемого в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

1) время и дата подачи заявления;

2) время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключа подписи;

3) идентификационные данные владельца сертификата ключа подписи, содержащиеся в поле "Субъект" (Subject) сертификата ключа подписи, статус которого требуется установить;

4) серийный номер сертификата ключа подписи, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата ключа подписи, которая предоставляется Заявителю.

Представление справки о статусе сертификата ключа подписи должно быть осуществлено не позднее 10 (десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

5.4. Предоставление сервисов службы актуальных статусов сертификатов и службы штампов времени

Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе сертификатов ключей подписи посредством сервиса службы актуальных статусов сертификатов (далее - САС). САС по запросам пользователей Удостоверяющего центра формирует и предоставляет OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата ключа подписи САС (оператора САС). OCSP-ответ признается действительным при одновременном выполнении следующих условий:

1) сертификат ключа подписи оператора САС действителен на момент формирования OCSP-ответа (при наличии достоверной информации о моменте подписания) или на момент проверки действительности указанного сертификата, если момент подписания OCSP-ответа не определен;

2) имеется положительный результат проверки принадлежности оператору САС электронной подписи, с помощью которой подписан OCSP-ответ, и подтверждено отсутствие изменений, внесенных в OCSP-ответ после его подписания (при этом проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с законодательством, и с использованием сертификата ключа подписи оператора САС);

3) сертификат ключа подписи оператора САС содержит в расширении "Расширенное использование ключа" (Extended Key Usage) область использования – "Подпись ответа службы OCSP" (1.3.6.1.5.5.7.3.9);

4) сертификат ключа подписи, статус которого установлен с использованием данного OCSP-ответа, издан Удостоверяющим центром и содержит в расширении "Расширенное использование ключа" (Extended Key Usage) или "Политики сертификата" (Certificate Policies) область использования "Пользователь службы актуальных статусов" (1.2.643.2.2.34.26).

Адрес обращения к службе актуальных статусов сертификатов Удостоверяющего центра – http://ocsp.citvo.ru/ocsp/ocsp.srf и http://ocsp.citvo.ru/ocsp2/ocsp.srf. Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых Удостоверяющим центром сертификатов ключей подписей.

Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса службы штампов времени (далее - СШВ). СШВ по запросам пользователей Удостоверяющего центра формирует и предоставляет в форме электронного документа штамп времени, подписанный электронной подписью с использованием сертификата ключа подписи СШВ (оператора СШВ).

Штамп времени, относящийся к заверенному электронной подписью электронному документу, признается действительным при одновременном выполнении следующих условий:

1) сертификат ключа подписи оператора СШВ действителен на момент формирования штампа времени (при наличии достоверной информации о моменте подписания) или на момент проверки действительности указанного сертификата, если момент подписания штампа времени не определен;

2) имеется положительный результат проверки принадлежности оператору СШВ электронной подписи, с помощью которой подписан штамп времени, и подтверждено отсутствие изменений, внесенных в штамп времени после его подписания (при этом проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с законодательством, и с использованием сертификата ключа подписи оператора СШВ);

3) сертификат ключа подписи оператора СШВ содержит в расширении "Расширенное использование ключа" (Extended Key Usage) область использования – "Подпись меток доверенного времени" (1.3.6.1.5.5.7.3.8);

4) сертификат ключа подписи, относящийся к электронной подписи электронного документа и к которому относится данный штамп времени, издан Удостоверяющим центром и содержит в расширении "Расширенное использование ключа" (Extended Key Usage) или "Политики сертификата" (Certificate Policies) область использования "Пользователь службы штампов времени" (1.2.643.2.2.34.25).

Адрес обращения к службе штампов времени Удостоверяющего центра – http://tsp.citvo.ru/tsp/tsp.srf.

5.5. Проверка электронной подписи в электронном документе

Подтверждение электронной подписи в электронном документе осуществляется Удостоверяющим центром в случае, если формат электронного документа с электронной подписью соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS) - RFC 3852. Решение о соответствии электронного документа с электронной подписью стандарту CMS принимает Удостоверяющий центр.

Подтверждение электронной подписи в электронном документе осуществляется Удостоверяющим центром на основании заявления на подтверждение электронной подписи в электронном документе в простой письменной форме, предоставляемого посредством почтовой либо курьерской связи.

Заявление на подтверждение электронной подписи в электронном документе должно содержать следующую информацию:

1) дата и время подачи заявления;

2) идентификационные данные Пользователя УЦ, содержащиеся в поле Subject сертификата ключа подписи, статус которого требуется установить;

3) содержащиеся в поле Subject сертификата ключа подписи идентификационные данные Пользователя УЦ, подлинность электронной подписи которого необходимо подтвердить в электронном документе;

4) время и дата формирования электронной подписи электронного документа;

5) время и дата, на момент наступления которых требуется установить подлинность электронной подписи.

Время доказывания достоверности даты и времени формирования электронной подписи в электронном документе возлагается на заявителя.

Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является носитель информации, содержащий следующие файлы:

1) сертификат ключа подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе;

2) 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).

Срок рассмотрения заявления на подтверждение электронной подписи в электронном документе составляет не более 10 (десяти) рабочих дней с момента его поступления в Удостоверяющий центр.

В случае отказа от подтверждения электронной подписи в электронном документе заявителю возвращается заявление на подтверждение электронной цифровой подписи в электронном документе с указанием причины отказа.

В случае принятия положительного решения по заявлению на подтверждение электронной подписи в электронном документе заявителю предоставляется ответ в письменной форме, заверенный подписью должностного лица Удостоверяющего центра и печатью Удостоверяющего центра.

Ответ содержит:

1) результат проверки электронной подписи в электронном документе;

2) детальный отчет по выполненной проверке (экспертизе).

Детальный отчет по выполненной проверке включает следующие обязательные компоненты:

3) время и место проведения проверки (экспертизы);

4) основания для проведения проверки (экспертизы);

5) сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность),

которым поручено проведение проверки (экспертизы);

6) вопросы, поставленные перед экспертом или комиссией экспертов;

7) объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);

8) содержание и результаты исследований с указанием примененных методов;

9) результаты исследований, выводы по поставленным вопросам и их обоснование;

10) иные сведения в соответствии с Законодательством Российской Федерации.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчету и служат его составной частью.

Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или собственноручными подписями членов экспертной комиссии.

В случае, если формат электронного документа с электронной подписью не соответствует стандарту криптографических сообщений CMS, то проведение экспертных работ по подтверждению подлинности электронной подписи осуществляется в рамках заключения отдельного договора (соглашения) с Удостоверяющим центром. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (акты, заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором (соглашением).

6. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

Ключ электронной подписи является конфиденциальной информацией Пользователя УЦ. Удостоверяющий центр не хранит и не создает копии ключей электронных подписей, изготавливаемых по соответствующим заявлениям Пользователей УЦ.

Не считается конфиденциальной информация, включаемая в издаваемые Удостоверяющим центром сертификаты ключей подписей, а также вносимая в Реестр сертификатов.

Персональные данные, включаемые в сертификаты ключей подписей, издаваемые Удостоверяющим центром, а также вносимые в Реестр сертификатов относятся к общедоступным персональным данным.

Удостоверяющий центр обеспечивают защиту конфиденциальной информации и персональные данных Пользователей УЦ – физических лиц и Пользователей сертификатов от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

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

7. СЕРТИФИКАТЫ КЛЮЧЕЙ ПОДПИСИ И СПИСКИ АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

7.1. Сертификаты ключей подписи

Удостоверяющий центр издает сертификаты ключей подписей формата X.509 версии 3 согласно рекомендациям "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (RFC 3280) и соответствующие требованиям к форме квалифицированного сертификата ключа подписи, установленным федеральный орган исполнительной власти в области обеспечения безопасности.

Программное обеспечение Удостоверяющего центра и Пользователей УЦ должно поддерживать данный формат сертификатов ключей подписи и обеспечивать возможность управления ими.

Перечень политик применения (с соответствующими объектными идентификаторами) определяющих сферу применения сертификатов ключей подписей, зарегистрированных в Удостоверяющем центре и включаемых в сертификаты ключей подписей, определяется

утверждаемыми в одностороннем порядке Удостоверяющим центром "Перечень политик применения, включаемых в сертификаты ключей проверки электронных подписей" и публикуемыми на сайте Удостоверяющего центра.

7.2. Списки аннулированных сертификатов

Удостоверяющий центр издает списки аннулированных сертификатов формата X.509 версии 2 согласно рекомендациям "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (RFC 3280).

Программное обеспечение Удостоверяющего центра и Пользователей УЦ должно поддерживать данный формат списков аннулированных сертификатов и обеспечивать возможность управления ими.

8. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Сроки действия ключей электронной подписи

8.1.1. Срок действия ключей электронной подписи Пользователей УЦ

Срок действия ключа электронной подписи и сертификата ключа подписи составляет 1 (один) год.

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

8.1.2. Срок действия ключа электронной подписи и сертификата ключа подписи Удостоверяющего центра

Срок действия ключа электронной подписи Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра, и для средства электронной подписи, с использованием которого данный закрытый ключ был сформирован. Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени формирования ключа электронной подписи Удостоверяющего центра.

Срок действия сертификата ключа подписи Удостоверяющего центра составляет максимально допустимый срок действия ключа подписи, включенного в сертификат, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра и для средства электронной подписи, с использованием которого данный ключ был сформирован.

8.2. Плановая смена ключей Удостоверяющего центра

Плановая смена ключа электронной подписи и соответствующего ему сертификата ключа подписи Удостоверяющего центра осуществляется за 1 (один) год до окончания срока действия сертификата ключа подписи Удостоверяющего центра.

Уведомление Пользователей УЦ о проведении смены сертификата ключа подписи Удостоверяющего центра осуществляется посредством размещения соответствующей информации на сайте Удостоверяющего центра.

Старый ключ электронной подписи Удостоверяющего центра используется до окончания срока его действия для формирования списков аннулированных сертификатов, изданных Удостоверяющим центром в период действия старого ключа электронной подписи Удостоверяющего центра.

8.3. Внеплановая смена ключей Удостоверяющего центра

Внеплановая смена ключа электронной подписи и сертификата ключа подписи Удостоверяющего центра выполняется в случае компрометации или угрозы компрометации ключа электронной подписи Удостоверяющего центра.

При этом сертификат ключа подписи Удостоверяющего центра аннулируется, Пользователи УЦ уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и/или публикации информации о компрометации на сайте Удостоверяющего центра. Все сертификаты ключей подписи, изданные с использованием скомпрометированного ключа электронной подписи Удостоверяющего центра, считаются аннулированными.

После аннулирования сертификата ключа подписи Удостоверяющего центра выполняется процедура внеплановой смены ключей электронной подписи и сертификата ключа подписи Удостоверяющего центра.

Все действовавшие на момент компрометации ключа электронной подписи

Удостоверяющего центра сертификаты ключей подписей подлежат внеплановой смене.

8.4. Компрометация ключей электронной подписи Пользователя УЦ

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

В случае компрометации Пользователь УЦ аннулирует сертификат ключа подписи (пункт 6.2.1 или 6.2.2 настоящего Регламента).

Пользователь УЦ осуществляет получение новых ключей электронной цифровой подписи в соответствии с пунктом 6.1 настоящего Регламента.

8.5. Требования к средствам электронной подписи

Применяемые средства электронной подписи должны обеспечивать работу с сертификатами ключей подписи формата X.509 версии 3, определенному рекомендациями "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (RFC 3280) и соответствовать требованиям к средствам электронной подписи устанавливаемым законодательством Российской Федерации.

8.6. Хранение документов

Документальный фонд Удостоверяющего центра хранится в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

В документальный фонд, формируемый Удостоверяющим центром и подлежащий архивному хранению, входят:

1) заявки на оказание услуг Удостоверяющего центра;
2) заявления о присоединении к Регламенту;
3) заявления об изготовлении ключей электронных подписей и сертификатов ключей подписей;
4) доверенности или иные документы, подтверждающие право уполномоченных представителей действовать от имени Пользователей УЦ;
5) заявления на аннулирование сертификатов ключей подписей.

Срок хранения документов в Удостоверяющем центре устанавливается в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется работниками Удостоверяющего центра в соответствии с приказом по уничтожению документов и в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

8.7. Обработка персональных данных

8.7.1. Цели обработки персональных данных

Обработка персональных данных Удостоверяющим центром осуществляется в целях исполнения функций и обязанностей удостоверяющих центров, предусмотренных Федеральным законом от 06 апреля 2011 г. N63-ФЗ "Об электронной подписи" и принимаемых в соответствии с ним подзаконных нормативных правовых актов.

8.7.2. Состав обрабатываемых персональных данных

Удостоверяющий центр обрабатывает следующие персональные данные Пользователей УЦ – физических лиц, включаемые в их сертификаты ключей подписей: фамилия, имя, отчество, страховой номер индивидуального лицевого счета, а также, при необходимости, адрес электронной

почты, идентификационный номер налогоплательщика, данные аттестата кадастрового инженера или другие данные по заявлению владельца сертификата.

Кроме того, в соответствии с п.1 ч.1 статьи 15 Федерального закона от 06 апреля 2011 г. N63-ФЗ "Об электронной подписи" обеспечивает хранение информации о реквизитах основного документа, удостоверяющего личность Пользователя УЦ - физического лица. В соответствии с Порядком ведения реестра Удостоверяющий центр включает данную информацию в Реестр сертификатов и обеспечивает доступ к нему с использованием информационно-телекоммуникационных сетей любому лицу в течение срока деятельности Удостоверяющего центра.

Заявители – юридические лица предоставляют в Удостоверяющий центр следующие персональные данные своих уполномоченных лиц, включаемые в сертификаты ключей подписей: фамилия, имя, отчество, место работы и должность, а также, при необходимости, адрес электронной почты, идентификационный номер налогоплательщика или другие данные по заявлению Заявителя.

Заявители – физические лица и уполномоченные лица юридических лиц, сведения о которых включаются в сертификаты ключей подписей, дают согласие на обработку (в том числе, на распространение) Удостоверяющим центром своих персональных данных, вносимых в сертификаты ключей подписей и включаемых в реестр квалифицированных сертификатов (делают эти персональные данные общедоступными).

Заявители - юридические лица самостоятельно получает согласие от своих уполномоченных лиц на предоставление в Удостоверяющий центр их персональных данных, порядок обработки которых определен в настоящем Регламенте.

Услуги по изготовлению сертификата ключа подписи не оказываются Удостоверяющим центром в случае не предоставления персональных данных, необходимых для изготовления сертификата ключа подписи.

8.7.3. Общие принципы обработки персональных данных

Обработка персональных данных осуществляется Удостоверяющим центром как с использованием средств вычислительной техники (автоматизированная обработка персональных данных), так и без использования таких средств.

Сбор персональных данных осуществляется при приеме в соответствии с настоящим положением форм заявлений, а также документов, подтверждающих сведения, вносимые в сертификаты ключей подписей.

Полученные персональные данные используются для изготовления сертификатов ключей подписей путем внесения данных в соответствующие поля сертификатов ключей подписей.

Удостоверяющий центр в соответствии с ч. 2 статьи 15 Федерального закона от 06 апреля 2011 г. и N63-ФЗ "Об электронной подписи" обеспечивает хранение полученных персональных данных в течение всего срока своей деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации.

В соответствии с ч.3 статьи 15 Федерального закона от 06 апреля 2011 г. и N63-ФЗ "Об электронной подписи" Удостоверяющий центр обязан обеспечить доступ любому лицу к выданным сертификатам ключей подписей, в том числе к содержащимся в них персональным данным.

Распространение общедоступных персональных данных владельцев сертификатов ключей подписей осуществляется путем передачи сертификатов ключей подписей по телекоммуникационным каналам связи и размещением на сайте и других информационных ресурсах Удостоверяющего центра в информационно-телекоммуникационной сети "Интернет".

8.7.4. Меры по обеспечению информационной безопасности, принимаемые Удостоверяющим центром при обработке персональных данных

Удостоверяющий центр принимает следующие меры по обеспечению информационной безопасности персональных данных, полученных и обрабатываемых в целях, определенных

настоящим Регламентом, от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных:

1) определяет угрозы безопасности персональных данных при их обработке в информационных системах;

2) применяет средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия;

3) устанавливает правила доступа к персональным данным, обрабатываемым в информационных системах;

4) обеспечивает аудит фактов несанкционированного доступа к персональным данным;

5) обеспечивает проведение оценки соответствия информационной системы Удостоверяющего центра (аттестации) в соответствии с законодательством об информации, информатизации и о защите информации;

6) выполняет резервное копирование персональных данных, обрабатываемых в информационных системах;

7) ведет учет машинных носителей персональных данных;

8) принимает необходимые организационные меры по обеспечению безопасности персональных данных, в том числе определяет список работников Удостоверяющего центра, допущенных к обработке персональных данных;

9) обеспечивает проведение регулярного контроля за соответствием принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем Удостоверяющего центра.

Приложение 1

Форма заявления о присоединении к Регламенту Удостоверяющего центра для физических лиц

Директору государственного бюджетного учреждения Волгоградской области "Центр информационных технологий Волгоградской области"

Заявление о присоединении к Регламенту оказания услуг Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта кем и когда выдан)

_____,
(адрес, контактные телефоны и e-mail)

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту оказания услуг Удостоверяющего центра ГБУ ВО "ЦИТ ВО" (далее - Регламент)), условия которого определены ГБУ ВО "ЦИТ ВО" и опубликованы по адресу http://www.citvo.ru/struct/ca/ecp/RegCA.pdf.

С Регламентом и приложениями к нему я ознакомлен (на), и обязуюсь соблюдать все положения указанного документа.

Соглашаюсь с тем, что изменения в Регламент вносятся в одностороннем порядке Удостоверяющим центром ГБУ ВО "ЦИТ ВО" в соответствии с п.2.3.6 Регламента.

В соответствии со ст. 9 Федерального закона от 27.07.2006 N152-ФЗ "О персональных данных" даю согласие на обработку моих персональных данных (далее - ПДн), перечень и порядок обработки которых определен в Регламенте, оператору - Государственному бюджетному учреждению Волгоградской области "Центр информационных технологий Волгоградской области" (далее - УЦ), расположенному по адресу: 400012 г. Волгоград, ул. Витимская, д. 15А, оф.403, в целях идентификации и аутентификации меня при изготовлении и обслуживании в соответствии с Федеральным законом от 06.04.2011 и N63-ФЗ "Об электронной подписи" (далее – Закон 63-ФЗ) сертификатов ключей подписи (далее - сертификат), владельцем которых я буду являться.

Я даю согласие УЦ на распространение (раскрытие неопределенному кругу лиц) в соответствии Законом 63-ФЗ моих ПДн, включаемых в сертификаты ключей подписей, владельцем которых я буду являться, а также включаемых УЦ в Реестр сертификатов.

Я уведомлен, о последствиях непредставления моих персональных данных, необходимых для изготовления сертификатов, и о том, что в случае отзыва моего согласия на обработку ПДн, ПДн, включаемые в сертификат и реквизиты основного документа, удостоверяющего личность, УЦ продолжит осуществлять их обработку в соответствии с Законом 63-ФЗ в течение всего срока деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами РФ.

_____ _____
ФИО подпись

"____" _____ 20____ г.

(заполняется Удостоверяющим центром ГБУ ВО "ЦИТ ВО")

Данное заявление зарегистрировано в реестре Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

Регистрационный N _____ от "_____" _____ 20___ г.

*Зарегистрировал: ___*_____ _____
подпись *ФИО*

Приложение 2

Форма заявления о присоединении к регламенту юридических лиц

Директору государственного бюджетного учреждения Волгоградской области "Центр информационных технологий Волгоградской области"

Заявление о присоединении к Регламенту оказания услуг Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

"____" _____ 20_ _г.

_____
(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 оказания услуг Удостоверяющего центра ГБУ ВО "ЦИТ ВО" (далее - Регламент), условия которого определены ГБУ ВО "ЦИТ ВО" и опубликованы по адресу http://www.citvo.ru/struct/ca/ecp/RegCA.pdf.

С Регламентом и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа.

Соглашаюсь с тем, что изменения в Регламент вносятся в одностороннем порядке Удостоверяющим центром ГБУ ВО "ЦИТ ВО" в соответствии с п.2.3.6 Регламента.

_____	_____	_____
(должность руководителя)	(подпись)	ФИО

М.П.

(заполняется Удостоверяющим центром ГБУ ВО "ЦИТ ВО")

Данное заявление зарегистрировано в реестре Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

Регистрационный N _____ от "_____" _____ 20___ г.

Зарегистрировал: _____ _____
подпись *ФИО*

Приложение 3

Форма заявки на оказание услуг Удостоверяющего центра

Директору государственного бюджетного учреждения
Волгоградской области
"Центр информационных технологий
Волгоградской области"

ЗАЯВКА
на оказание услуг Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

_____
полное наименование юридического лица, включая организационно-правовую форму

в лице_____,
должность, фамилия, имя, отчество

действующего на основании _____, просит изготовить ключи и (или) сертификаты ключей электронной подписи в соответствии с прилагаемыми заявлениями в количестве ___ *(цифрами и прописью)* шт.

Представитель от организации:

_____
Должность, ФИО, тел., email (обязательно)

В соответствии с ч.3 ст.6 Федерального закона от 27 июля 2006 г. N152-ФЗ "О персональных данных" получено согласие уполномоченных лиц на передачу их персональных данных для обработки в Удостоверяющем центре ГБУ ВО "ЦИТ ВО", цели которой, а также состав и перечень действий с персональными данными определены Регламентом Удостоверяющего центра ГБУ ВО "ЦИТ ВО".

Реквизиты юридического лица:
ОГРН:_____
Адрес:_____
телефон _____, факс _____,
ИНН _____ КПП _____
Р/с.: _____ в _____
К/с.: _____; БИК _____

К заявке прилагаются (указать перечень предоставляемых документов):
1.
2.
…..

"____" _____ 20__г. _____/_____
подпись ФИО

М.П.

(заполняется Удостоверяющим центром ГБУ ВО "ЦИТ ВО")

Данное заявление зарегистрировано в реестре Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

Регистрационный N _____ от "_____" _____ 20___ г.
Зарегистрировал: _____ _____
подпись ФИО

Приложение 4

Форма заявления юридического лица на изготовление ключей электронной подписи и сертификата ключа подписи

Директору государственного бюджетного
учреждения Волгоградской области "Центр
информационных технологий
Волгоградской области"

ЗАЯВЛЕНИЕ
на создание квалифицированного сертификата ключа проверки электронной подписи для юридических лиц, содержащего в качестве владельца сертификата наряду с наименованием юридического лица физическое лицо

_____
Наименование организации, включая организационно-правовую форму

в лице _____

_____
Должность, фамилия, имя, отчество

действующего на основании _____

ИНН_____ОГРН_____

Прошу изготовить ключи электронной подписи и (или) квалифицированный сертификат ключа проверки электронной подписи в соответствии со следующей информацией:

В качестве владельца сертификата ключа проверки электронной подписи, наряду с указанием в сертификате наименования нашей организации, прошу указать следующего полномочного представителя, действующего от ее имени – пользователя удостоверяющего центра:

Ограничения на использование сертификата ключа подписи:

	Для подписания электронных документов в АСЭД	
	Электронная подпись уполномоченного / юридического (подчеркнуть) лица в государственной информационной системе Волгоградской области «Электронный бюджет Волгоградской области»	
	для использования в Единой информационно-аналитической системе Федеральной службы по тарифам (ЕИАС ФСТ)	
	Для получения госуслуг Росреестра[1]: _____	
	Для юридического лица для подписания электронных документов при межведомственном взаимодействии СМЭВ УЛ / СМЭВ ЮЛ (подчеркнуть)	
	Для использования в Автоматизированной системе АС Бюджет и удаленном рабочем месте АС УРМ (НПО КРИСТА)	
	Для использования в ИС Администрации Волгограда[2]:_____	
	Для доступа к Порталу Росфинмониторинг	

[1] Указывается наименование субъекта получения ЭП, определяемой Приложением 4 к **распоряжению** Федеральной службы государственной регистрации, кадастра и картографии от 27 марта 2014 г. N Р/3

[2] Указывается субъект-получатель КСКПЭП, определяемый Приложением 2 Постановления администрации Волгограда от 12.08.2015 № 1166

	Не устанавливаются	

2.Сведения об уполномоченном лице

Фамилия, имя отчество:

Подразделение:

Должность:

Страховой номер индивидуального лицевого счета уполномоченного лица:

- -

3.Адрес электронной почты (если не указываются сведения об уполномоченном лице, то необходимо указать адрес электронной почты организации)

4.Наименование и версия средства электронной подписи:

.Предоставление ключевых носителей (отметить, если требуется):

6.Предоставление копии сертификата ключа подписи на бумажном носителе (отметить, если требуется):

7.Дополнительные сведения для доступа уполномоченного лица к информационным ресурсам ЕЦОД (указать при необходимости):

7.1. Наименование информационной системы:

7.2. UPN учетной записи пользователя в едином домене ОИВ ВО:

Настоящим_____

Фамилия, имя, отчество

_____

Дата рождения

_____

Паспорт, серия и номер

_____Дата

выдачи Код подразделения Кем выдан

соглашается с обработкой своих персональных данных ГБУ ВО «ЦИТ ВО» и признает, что персональные данные, заносимые в сертификаты ключей проверки электронной подписи, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь удостоверяющего центра
ГБУ ВО «ЦИТ ВО»

_____ _____

ФИО Подпись

«___» _____ 20___ г.

_____ _____

Должность, ФИО руководителя организации Подпись

«___» _____ 20___ г. М.П.

_____

Достоверность сведений, указанных в заявлении, подтверждаю: (заполняется сотрудником УЦ)

_____ _____

подпись *ФИО*

Приложение 5

Форма заявления физического лица на изготовление ключа электронной подписи и сертификата ключа подписи

Директору государственного бюджетного учреждения
Волгоградской области "Центр информационных
технологий Волгоградской области"

Заявление на изготовление
ключей электронной подписи и сертификата ключа подписи

Я,

_____
(фамилия, имя, отчество)

_____
(серия и номер паспорта кем и когда выдан)

_____,
прошу изготовить ключи электронной подписи и (или) сертификат ключа электронной подписи в соответствии со следующей информацией:

1. Ограничения на использование сертификата ключа подписи:

1.	Для получения госуслуг Росреестра[1]: _____	
2.	Для доступа к Порталу Росфинмониторинг	
3.	Для использования в Единой информационно-аналитической системе Федеральной службы по тарифам (ЕИАС ФСТ)	
4.	Нет	

2. Сведения о владельце сертификата

Фамилия, имя отчество:

Страховой номер индивидуального лицевого счета

			-				-				

3. Адрес электронной почты

4. Наименование и версия средства электронной подписи:

5. Предоставление ключевых носителей (отметить, если требуется): ☐
6. Предоставление копии сертификата ключа подписи на бумажном носителе (отметить, если требуется): ☐
7. Дополнительные сведения (указать при необходимости):

7.1 ИНН:

7.2 Номер аттестата кадастрового инженера:

7.3 номер ОГРНИП:

[1] Указывается наименование субъекта получения ЭП, определяемой Приложением 4 к распоряжению Федеральной службы государственной регистрации, кадастра и картографии от 27 марта 2014 г. N Р/3

К заявлению прилагаются (указать перечень предоставляемых документов):

1.
2.
3.

"____" _____ 201_г. _____/_____

подпись ФИО

(заполняется Удостоверяющим центром ГБУ ВО "ЦИТ ВО")

Данное заявление зарегистрировано в реестре Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

Регистрационный N _____ от "_____" _____ 20___ г.
Зарегистрировал: _____ _____
подпись ФИО

Приложение 6

Форма заявления на аннулирование сертификата ключа подписи юридического лица

Директору государственного бюджетного учреждения
Волгоградской области "Центр информационных
технологий Волгоградской области"

Заявление
на аннулирование сертификата ключа подписи

_____
полное наименование организации, включая организационно-правовую форму

в лице __ _____,
должность

_____,
фамилия, имя, отчество

действующего на основании _____

просит аннулировать сертификат ключа подписи с серийным номером: _____

в связи с[1] _____
причина отзыва сертификата

"____" _____ 20__г. _____/_____
подпись ФИО

М.П.

(заполняется Удостоверяющим центром ГБУ ВО "ЦИТ ВО")

Данное заявление зарегистрировано в реестре Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

Регистрационный N _____ от "_____" _____ 20___ г.
Зарегистрировал: _____ _____
подпись ФИО

[1] Указывается причина: «Выход из строя ключевого носителя», «Компрометация ключа», «Прекращение полномочий уполномоченного лица», «Изменение идентификационных данных/реквизитов владельца»

Приложение 7

Форма заявления на аннулирование сертификата ключа подписи физического лица

Директору государственного бюджетного учреждения
Волгоградской области "Центр информационных
технологий Волгоградской области"

Заявление
на аннулирование сертификата ключа подписи

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта кем и когда выдан)

прошу аннулировать мой сертификат ключа подписи с серийным номером: _____

в связи с[1] _____
причина отзыва сертификата

"____" _____ 20__г. _____/_____
подпись ФИО

(заполняется Удостоверяющим центром ГБУ ВО "ЦИТ ВО")

Данное заявление зарегистрировано в реестре Удостоверяющего центра ГБУ ВО "ЦИТ ВО"

Регистрационный N _____ от "_____" _____ 20___ г.
Зарегистрировал: _____ _____
подпись ФИО

[1] Указывается причина: «Выход из строя ключевого носителя», «Компрометация ключа», «Прекращение полномочий уполномоченного лица», «Изменение идентификационных данных/реквизитов владельца»

Приложение 8

Памятка об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки

1. Нарушение конфиденциальности (компрометация) ключа электронной подписи является основным риском, связанным с использованием электронных подписей. Нарушением конфиденциальности считается подозрение или факт доступа неуполномоченного лица к ключу электронной подписи. К нарушению конфиденциальности также относятся:

– утрата ключевого носителя, на котором записан ключ электронной подписи, в том числе, с последующим обнаружением;

– доступ посторонних лиц к ключевой информации;

– нарушение целостности печатей на хранилище носителя ключевой информации;

– утрата ключей от хранилища в момент нахождения в них носителя ключевой информации, в том числе с последующим обнаружением ключей.

2. Владельцы сертификатов ключей проверки электронных подписей обязаны соблюдать меры, необходимые для обеспечения безопасности электронных подписей и их проверки:

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

– хранить в тайне ПИН-код ключевого носителя, на который записан ключ электронной подписи;

– осуществлять работу со средствами электронной подписи в помещениях с регламентированным доступом, которые должны иметь прочные входные двери с замками, гарантирующими их надежное закрытие в нерабочее время;

– хранить ключевые носители в шкафах (ящиках, хранилищах) индивидуального пользования, оборудованных приспособлениями для опечатывания;

– прекратить использование и немедленно обратиться в удостоверяющий центр с заявлением о прекращении действия сертификата ключа подписи в случае нарушения конфиденциальности или необратимого искажения ключа электронной подписи;

– применять для формирования электронной подписи действующий ключ электронной подписи;

– применять ключ электронной подписи в соответствии с правоотношениями, указанными в соответствующем данному ключу сертификате ключа подписи;

– не использовать ключ электронной подписи, связанный с сертификатом ключа подписи, заявление о прекращении действия которого подано в удостоверяющий центр;

– не использовать ключ электронной подписи, связанный с сертификатом ключа подписи, который аннулирован или действие которого прекращено;

– использовать для создания и проверки электронной подписи сертифицированные по требованиям безопасности информации средства электронной подписи.

Владельцы сертификатов ключей проверки электронных подписей несут персональную ответственность за сохранность ключа электронной подписи.