

УТВЕРЖДАЮ

Директор Государственного бюджетного
учреждения «Центр информационных
технологий Волгоградской области»



А.П. Внуков

«20» января 2016 г.

Регламент
оказания услуг Удостоверяющего центра
Государственного бюджетного учреждения
«Центр информационных технологий Волгоградской области»
Редакция 2.5

Содержание

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	4
2. ОБЩИЕ ПОЛОЖЕНИЯ	9
2.1. Сведения об Удостоверяющем центре	9
2.2. Контактная информация	9
2.3. Регламент оказания услуг Удостоверяющего центра	10
2.3.1. Идентификация Регламента.....	10
2.3.2. Статус Регламента	10
2.3.3. Распространение Регламента.....	11
2.3.4. Присоединение к Регламенту	11
2.3.5. Область применения Регламента	11
2.3.6. Порядок утверждения и внесения изменений в Регламент	12
2.3.7. Прекращение действия Регламента	13
2.4. Услуги, предоставляемые Удостоверяющим центром	13
2.5. Вознаграждение Удостоверяющего центра	14
3. ПРАВА И ОБЯЗАННОСТИ	14
3.1. Обязанности Удостоверяющего центра	14
3.2. Обязанности Пользователей УЦ	17
3.3. Права Удостоверяющего центра	19
3.4. Права Пользователей УЦ	19
4. РАЗРЕШЕНИЕ СПОРОВ	21
5. ОТВЕТСТВЕННОСТЬ	22
6. ПРОЦЕДУРЫ И МЕХАНИЗМЫ	23
6.1. Изготовление сертификата ключа подписи	23
6.2. Прекращение действия сертификата ключа подписи	26
6.2.1. Порядок аннулирования сертификата ключа подписи по заявлению, подаваемому в виде документа на бумажном носителе.....	28
6.2.2. Порядок аннулирования сертификата ключа подписи по заявлению, подаваемому в форме электронного документа	29
6.3. Предоставление информации о статусе сертификата ключа подписи	30
6.4. Предоставление сервисов службы актуальных статусов сертификатов и службы штампов времени	30
6.5. Проверка электронной подписи в электронном документе	33
7. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ	36
8. СЕРТИФИКАТЫ КЛЮЧЕЙ ПОДПИСИ И СПИСКИ АННУЛИРОВАННЫХ СЕРТИФИКАТОВ	37
8.1. Сертификаты ключей подписи	37
8.2. Списки аннулированных сертификатов	37
9. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	38
9.1. Сроки действия ключей электронной подписи	38
9.1.1. Срок действия ключей электронной подписи Пользователей УЦ.....	38

9.1.2. Срок действия ключа электронной подписи и сертификата ключа подписи Удостоверяющего центра.....	38
9.2. Плановая смена ключей Удостоверяющего центра	38
9.3. Внеплановая смена ключей Удостоверяющего центра	39
9.4. Компрометация ключей электронной подписи Пользователя УЦ	40
9.5. Требования к средствам электронной подписи	40
9.6. Хранение документов.....	40
9.7. Обработка персональных данных.....	41
9.7.1. Цели обработки персональных данных.....	41
9.7.2. Состав обрабатываемых персональных данных.....	41
9.7.3. Общие принципы обработки персональных данных	42
9.7.4. Меры по обеспечению информационной безопасности, принимаемые Удостоверяющим центром при обработке персональных данных	43
Приложение 1. Форма заявления о присоединении к Регламенту Удостоверяющего центра для физических лиц.....	45
Приложение 2. Форма заявления о присоединении к регламенту юридических лиц.....	46
Приложение 3. Форма заявки на оказание услуг Удостоверяющего центра	47
Приложение 4. Форма заявления юридического лица на изготовление ключей электронной подписи и сертификата ключа подписи	48
Приложение 5. Форма заявления физического лица на изготовление ключа электронной подписи и сертификата ключа подписи	50
Приложение 6. Примерная форма доверенности на право действовать от имени юридического лица.....	51
Приложение 7. Примерная форма доверенности на право действовать от имени физического лица	52
Приложение 8. Форма заявления на аннулирование сертификата ключа подписи юридического лица.....	53
Приложение 9. Форма заявления на аннулирование сертификата ключа подписи физического лица	54

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Владелец сертификата ключа проверки электронной подписи (Пользователь УЦ) - лицо, которому Удостоверяющим центром в соответствии с Федеральным законом от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" документом выдан сертификат ключа подписи.

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 проверки электронной подписи (квалифицированный сертификат, сертификат ключа подписи) - электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром и подтверждающие принадлежность ключа проверки электронной 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 (время Московское) 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. № 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 проверки электронной подписи.

Удостоверяющий центр – Государственное бюджетное учреждение «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 лица, 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.

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

- 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;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- ключ проверки электронной подписи указан в сертификате ключа

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.

проверки электронной 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. №63-ФЗ «Об электронной подписи».

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 проверки электронной 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)».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Сведения об Удостоверяющем центре

Удостоверяющий центр является юридическим лицом, зарегистрированным в соответствии с законодательством в городе Волгограде.

Удостоверяющий центр осуществляет свою деятельность на основании следующих лицензий:

1. Лицензия Управления Федеральной службы безопасности Российской Федерации по Волгоградской области № 93-У от 10 мая 2012г. на осуществление деятельности по предоставлению услуг в области шифрования информации;

2. Лицензия Управления Федеральной службы безопасности Российской Федерации по Волгоградской области № 91-Р от 10 мая 2012г. на осуществление деятельности по распространению шифровальных (криптографических) средств;

3. Лицензия Управления Федеральной службы безопасности Российской Федерации по Волгоградской области № 92-Х от 10 мая 2012г. на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Объектный идентификатор Удостоверяющего центра в российском сегменте мирового пространства идентификаторов: 1.2.643.3.122.

2.2. Контактная информация

Полное наименование организации: Государственное бюджетное учреждение «Центр информационных технологий Волгоградской области».

Сокращенное наименование организации: ГБУ «ЦИТ ВО».

Юридический адрес: 400131 г. Волгоград, ул.Новороссийская д.2к.

Фактический адрес: 400131 г. Волгоград, ул.Новороссийская д.2к.

Контактная информация:

Техническая поддержка: (8442) 55-19-85, (8442)55-19-86.

Служба регистрации Удостоверяющего центра: (8442) 55-19-84.

Факс: (8442) 55-19-90 (факс).

e-mail: ca@volganet.ru

Сайт: <http://ca.citvo.ru>

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 «Центр информационных технологий Волгоградской области», Редакция 2.4.

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://ca.citvo.ru/Portals/2/Files/regdocs/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 №1 – для физических лиц, №2 – для юридических лиц).

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 по истечении 10 (десяти) суток 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).

2.4. Услуги, предоставляемые Удостоверяющим центром

В процессе своей деятельности Удостоверяющий центр:

- создает сертификаты ключей подписей, устанавливает сроки их действия и выдает Заявителям;
- создает по обращениям Заявителей ключи электронных подписей и ключи проверки электронных подписей (с гарантией сохранения в тайне ключа электронной подписи);
- аннулирует выданные сертификаты ключей подписей;
- предоставляет по обращению Заявителей средства электронной подписи;
- ведет Реестр сертификатов и обеспечивает доступ организаций к

информации, содержащейся в нем, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;

- осуществляет по обращениям Заявителей проверку электронных подписей;

- оказывает консультации по вопросам применения электронной подписи;

- обеспечивает доступ любому лицу с использованием информационно-телекоммуникационной сети «Интернет» к перечню политик применения выдаваемых сертификатов ключей подписей, описывающих их юридическую сферу применения;

- осуществляет иную связанную с использованием электронной подписи деятельность.

2.5. Вознаграждение Удостоверяющего центра

Стоимость, сроки и порядок расчетов за оказанные услуги Удостоверяющего центра регулируются договором между Сторонами.

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.

3. ПРАВА И ОБЯЗАННОСТИ

3.1. Обязанности Удостоверяющего центра

Удостоверяющий центр обязан:

- 1) при выдаче сертификата ключа подписи предоставить Пользователю УЦ сертификат ключа подписи Удостоверяющего центра в электронной форме;
- 2) использовать ключ подписи Удостоверяющего центра только для подписания издаваемых им сертификатов ключей подписей и списков аннулированных сертификатов;
- 3) обеспечить соответствие выдаваемых сертификатов ключей подписей требованиям, устанавливаемым федеральным органом исполнительной власти в области обеспечения безопасности, к форме квалифицированного сертификата ключа проверки электронной подписи;
- 4) информировать в письменной форме заявителей 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;
- 5) при выдаче сертификата ключа подписи ознакомить заявителя под расписку с информацией, содержащейся в сертификате ключа подписи;
- 6) отказать заявителю в создании квалифицированного сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения квалифицированного сертификата ключа проверки электронной подписи;
- 7) отказать заявителю в создании квалифицированного сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в Реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения квалифицированного сертификата ключа проверки электронной подписи.
- 8) обеспечивать актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- 9) обеспечивать любому лицу безвозмездный доступ с использованием информационно-телекоммуникационной сети «Интернет» к Реестру

сертификатов в любое время в течение срока деятельности Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами;

10) предоставлять безвозмездно любому лицу по его обращению информацию, содержащуюся в Реестре сертификатов, в том числе информацию об аннулировании сертификата ключа подписи в форме выписки из Реестра сертификатов почтовым отправлением в срок, не превышающий пяти рабочих дней со времени обращения, или с использованием служб электронной почты в информационно-телекоммуникационной сети «Интернет» в срок не превышающий 24 часов со времени обращения (по выбору лица, обратившегося за получением информации из Реестра сертификатов);

11) обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей до их передачи Заявителю;

12) размещать (публиковать) актуальный список аннулированных сертификатов по адресам в информационно-телекоммуникационной сети «Интернет», указываемым в выпускаемых сертификатах ключей подписей в рабочие дни ежедневно, а в случаях прекращения действия сертификата ключа подписи до указанного в нем срока окончания действия – в течение 15 (пятнадцати) минут после получения Удостоверяющим центром информации о событии, повлекшим необходимость досрочного прекращения действия сертификата ключа подписи;

13) соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

14) хранить в течение всего срока деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, в форме, позволяющей проверить целостность и достоверность, следующую информацию:

– реквизиты основного документа, удостоверяющего личность Пользователя УЦ - физического лица

– сведения о наименовании, номере и дате выдачи документа,

подтверждающего право лица, выступающего от имени Заявителя - юридического лица, обращаться за получением сертификата ключа подписи;

– сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия Пользователя УЦ действовать по поручению третьих лиц, если информация о таких полномочиях Пользователя УЦ включена в сертификат ключа подписи.

15) принимать меры по защите ключа электронной подписи уполномоченного лица Удостоверяющего центра от несанкционированного доступа;

16) 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;

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

3.2. Обязанности Пользователей УЦ

Пользователи УЦ обязаны:

1) для получения сертификата ключа подписи предоставить в Удостоверяющий центр документы, подтверждающие сведения, вносимые в сертификаты ключей подписей, либо их копии, надлежащим образом заверенные;

2) уведомить Удостоверяющий центр о внесении изменений в документы, на основании которых Удостоверяющим центром были выпущены сертификаты ключей подписей Пользователя УЦ в течение не более чем одного рабочего дня со дня внесения изменений и по требованию Удостоверяющего центра предоставить их течение 5 (пяти) рабочих дней с момента регистрации изменений;

3) при получении сертификата ключа подписи ознакомиться под расписку с информацией, содержащейся в сертификате ключа подписи;

- 4) обеспечивать конфиденциальность ключей электронных подписей;
- 5) уведомить Удостоверяющий центр о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- 6) не использовать ключ электронной подписи и обратиться в порядке, установленном настоящим Регламентом, в Удостоверяющий центр для прекращения действия соответствующего сертификата ключа подписи при внесении изменений в документы, на основании которых Удостоверяющим центром был выпущен сертификат ключа подписи или при компрометации ключа электронной подписи;
- 7) использовать электронную подпись в соответствии с политиками применения (ограничениями), содержащимися в сертификате ключа подписи (при их наличии);
- 8) не использовать ключ электронной подписи, связанный с сертификатом ключа подписи, заявление на аннулирование которого подано в Удостоверяющий центр;
- 9) использовать для создания и проверки электронных подписей, создания ключей электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;
- 10) 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.

Пользователь УЦ – юридическое лицо также обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. №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.

3.3. Права Удостоверяющего центра

Удостоверяющий центр имеет право:

1) выдавать сертификаты ключей подписей в электронной форме и (или) на бумажном носителе;

2) отказать в аннулировании сертификата ключа подписи, поданного Пользователем УЦ, в случае ненадлежащего оформления заявления на аннулирование сертификата ключа подписи.

3) отказать Заявителю в изготовлении сертификата ключа подписи в случае:

1) неприсоединения Заявителя к Регламенту;

2) ненадлежащего оформления или непредставления необходимых документов;

3) отказа предоставления согласия субъекта персональных данных на обработку его персональных данных Удостоверяющим центром в целях изготовления сертификатов ключей подписей.

3.4. Права Пользователей УЦ

Пользователь УЦ имеет право:

1) при получении сертификата ключа подписи получить его копию на бумажном носителе, заверенную Удостоверяющим центром;

2) на получение от Удостоверяющего центра информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром, на определенный момент времени;

3) обратиться в Удостоверяющий центр за подтверждением подлинности электронной подписи в электронном документе, сформированной с использованием сертификата ключа подписи, изданного Удостоверяющим центром;

4) обратиться в Удостоверяющий центр за подтверждением подлинности

электронной подписи уполномоченного лица Удостоверяющего центра в изготовленных Удостоверяющим центром сертификатах ключей подписи;

5) обратиться в Удостоверяющий центр за получением (приобретением) средств электронной подписи;

6) на получение от Удостоверяющего центра подтверждения аннулирования сертификата ключа подписи.

4. 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.

5. ОТВЕТСТВЕННОСТЬ

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.

6. ПРОЦЕДУРЫ И МЕХАНИЗМЫ

6.1. Изготовление сертификата ключа подписи

Удостоверяющий центр осуществляет изготовление сертификата ключа подписи только в том случае, если Заявитель присоединился к Регламенту в соответствии с пунктом 1.3.4 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://ca.citvo.ru>.

Срок рассмотрения обращения Заявителя на оказание услуги по изготовлению сертификата ключа подписи составляет не более 2 (двух) часов 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, действующим на основании доверенности, подтверждающей его полномочия осуществлять взаимодействие с Удостоверяющим центром (примерная форма доверенности приведена в Приложении 7 к настоящему Регламенту).

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, страховое свидетельство государственного пенсионного страхования, идентификационный номер налогоплательщика Заявителя - физического лица, а также основной государственный регистрационный номер записи о государственной регистрации Заявителя - физического лица в качестве индивидуального предпринимателя или учредительные документы, документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц и свидетельство о постановке на учет в налоговом органе Заявителя - юридического лица;

2) надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);

3) доверенность или иной документ, подтверждающий право Заявителя действовать от имени других лиц.

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 принятия или отказе (с указанием причины) принятия к обработке, проставляет текущую дату, и заверяет своей подписью;

5) при положительном результате проверки 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) ознакомливает 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.

6.2. 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, 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 владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- 7) в случае, если установлено, что содержащийся в сертификате ключа проверки электронной подписи ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- 8) вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит

недостоверную информацию.

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

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 проверки электронной 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 проверки электронной 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. 6.1 настоящего Регламента.

6.2.1. 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.

6.2.2. 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 ca@volganet.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.

6.3. 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.

6.4. 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>. 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>.

6.5. 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.

Бремя 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);
- б) 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).

7. 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.

8. СЕРТИФИКАТЫ КЛЮЧЕЙ ПОДПИСИ И СПИСКИ АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

8.1. 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 проверки электронной подписи, установленным федеральным органом 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.

8.2. 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.

9. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Сроки действия ключей электронной подписи

9.1.1. 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.

9.1.2. 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 проверки электронной подписи, включенного в сертификат, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра и для средства электронной подписи, с использованием которого данный ключ был сформирован..

9.2. 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.

9.3. 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.

9.4. 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.

9.5. 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.

9.6. 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.

9.7. Обработка персональных данных

9.7.1. 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. №63-ФЗ «Об электронной подписи» и принимаемых в соответствии с ним подзаконных нормативных правовых актов.

9.7.2. 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. №63-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).

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.

9.7.3. 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 №63-ФЗ «Об электронной подписи» обеспечивает хранение полученных персональных данных в течение всего срока своей деятельности.

В соответствии с ч.3 статьи 15 Федерального закона от 06 апреля 2011 г. и №63-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».

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

Удостоверяющим центром принимаются 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) по требованиям защиты конфиденциальной 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
«Центр информационных технологий Волгоградской области»

Заявление о присоединении к Регламенту оказания услуг Удостоверяющего центра ГБУ «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 «ЦИТ ВО» (далее - Регламент), условия которого определены ГБУ «ЦИТ ВО» и опубликованы по адресу <http://ca.citvo.ru/Portals/2/Files/regdocs/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 «ЦИТ ВО» в соответствии с п.2.3.6 Регламента.

В соответствии со ст. 9 Федерального закона от 27.07.2006 №152-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 «Центр информационных технологий Волгоградской области» (далее - УЦ), расположенному по адресу: 400131, г. Волгоград, ул. Новороссийская, д. 2к в целях идентификации и аутентификации меня при изготовлении и обслуживании в соответствии с Федеральным законом от 06.04.2011 и №63-ФЗ «Об электронной подписи» (далее – 63-ФЗ) сертификатов ключей подписи (далее - сертификат), владельцем которых я буду являться.

Я даю согласие УЦ на распространение (раскрытие неопределенному кругу лиц) в соответствии 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 63-ФЗ в течение всего срока деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами РФ.

И.О.Фамилия

подпись

« ____ » _____ 20 ____ г.

_____ (заполняется Удостоверяющим центром ГБУ «ЦИТВО»)

Данное Заявление зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от « ____ » _____ 20 ____ г.

Зарегистрировал: _____

подпись

Фамилия И.О.

Приложение 2. Форма заявления о присоединении к регламенту юридических лиц

Директору Государственного бюджетного учреждения
«Центр информационных технологий Волгоградской области»

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

« ____ » _____ 201_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 «ЦИТ ВО» (далее - Регламент), условия которого определены ГБУ «ЦИТ ВО» и опубликованы по адресу <http://ca.citvo.ru/Portals/2/Files/regdocs/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 «ЦИТ ВО» в соответствии с п.2.3.6 Регламента.

(должность руководителя)

(подпись)

И.О.Фамилия

М.П.

(заполняется Удостоверяющим центром ГБУ «ЦИТВО»)

Данное Заявление зарегистрировано в реестре Удостоверяющего центра.
Регистрационный № _____ от « ____ » _____ 20__ г.

Зарегистрировал: _____
подпись _____ Фамилия И.О. _____

Приложение 3. Форма заявки на оказание услуг Удостоверяющего центра

Директору Государственного бюджетного учреждения
«Центр информационных технологий
Волгоградской области»

ЗАЯВКА на оказание услуг Удостоверяющего центра ГБУ «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. №152-ФЗ «О персональных данных» получено согласие уполномоченных лиц на передачу их персональных данных для обработки в Удостоверяющем центре ГБУ «ЦИТ ВО», цели которой, а также состав и перечень действий с персональными данными определены Регламентом Удостоверяющего центра ГБУ «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 «ЦИТ ВО»)

Данная заявка зарегистрирована в реестре Удостоверяющего центра ГБУ «ЦИТ ВО».

Регистрационный № _____ от « ____ » _____ 20__ г.

Зарегистрировал: _____ И.О.Фамилия
подпись

Приложение 6. Примерная форма доверенности на право действовать от имени юридического лица

ДОВЕРЕННОСТЬ

(наименование населенного пункта)

« _____ года».
(дата, месяц, год – прописью)

Настоящей доверенностью, _____
(полное наименование организации)

в лице _____,
(должность, ФИО)

действующего на основании _____,

уполномочивает _____,
(ФИО уполномоченного лица)

паспорт № _____ серия _____ выдан _____
(кем и когда выдан)

совершать следующие действия:

1. Передавать в Государственное бюджетное учреждение «Центр информационных технологий Волгоградской области» комплекты документов для создания ключей электронной подписи и (или) сертификатов ключей подписей;
2. Получать в Государственном бюджетном учреждении «Центр информационных технологий Волгоградской области» ключи электронной подписи и сертификаты ключей подписей;
3. Ознакомиться с информацией, содержащейся в получаемых сертификатах ключей подписей;
4. Получать в Государственном бюджетном учреждении «Центр информационных технологий Волгоградской области» средства криптографической защиты информации (средства электронной подписи);
5. Получать руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи;
6. Передавать в Государственное бюджетное учреждение «Центр информационных технологий Волгоградской области» заявления на аннулирование сертификатов ключей подписей;
7. Расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность выдана по « _____ » _____ 20____ г. без права передоверия.

Собственноручную подпись _____ / _____ удостоверяю.
(Подпись доверенного лица) (ФИО доверенного лица)

(должность руководителя)

(подпись)

ФИО

М.П.

Приложение 7. Примерная форма доверенности на право действовать от имени физического лица

ДОВЕРЕННОСТЬ*

(наименование населенного пункта)

«_____ года».
(дата, месяц, год – прописью)

Я, _____
(фамилия, имя, отчество)

уполномочиваю _____,
(ФИО уполномоченного лица)

паспорт № _____ серия _____ выдан _____
(кем и когда выдан)

совершать следующие действия:

1. Передавать в Государственное бюджетное учреждение «Центр информационных технологий Волгоградской области» комплекты документов для создания ключей электронной подписи и (или) сертификатов ключей подписей;
2. Получать в Государственном бюджетном учреждении «Центр информационных технологий Волгоградской области» ключи электронной подписи и сертификаты ключей подписей;
3. Ознакомиться с информацией, содержащейся в получаемых сертификатах ключей подписей;
4. Получать в Государственном бюджетном учреждении «Центр информационных технологий Волгоградской области» средства криптографической защиты информации (средства электронной подписи);
5. Получать руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи;
6. Передавать в Государственное бюджетное учреждение «Центр информационных технологий Волгоградской области» заявления на аннулирование сертификатов ключей подписей;
7. Расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность выдана по «___» _____ 20___ г. без права передоверия.

(подпись)

ФИО

* Настоящая Доверенность должна быть заверена нотариусом

Приложение 8. Форма заявления на аннулирование сертификата ключа подписи юридического лица

Директору Государственного бюджетного учреждения
«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 с¹ _____
причина отзыва сертификата

« _____ » _____ 20__ г. _____ / _____
подпись ФИО

М.П.

_____ (заполняется Удостоверяющим центром ГБУ «ЦИТ ВО»)

Данное Заявление зарегистрировано в реестре Удостоверяющего центра ГБУ «ЦИТ ВО»

Регистрационный № _____ от « _____ » _____ 20__ г.

Зарегистрировал: _____, _____
подпись Фамилия И.О.

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

Приложение 9. Форма заявления на аннулирование сертификата ключа подписи физического лица

Директору Государственного бюджетного учреждения
«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 с¹ _____
причина отзыва сертификата

« ____ » _____ 20__ г.

_____ / _____
подпись

_____ / _____
ФИО

_____ (заполняется Удостоверяющим центром ГБУ «ЦИТ ВО»)

Данное Заявление зарегистрировано в реестре Удостоверяющего центра ГБУ «ЦИТ ВО»

Регистрационный № _____ от « ____ » _____ 20__ г.

Зарегистрировал: _____
подпись

_____ / _____
Фамилия И.О.

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