«Утверждаю»

Генеральный директор

ООО Телекоммуникационная компания «Контакт»

/Лантюхов М.Н./

“ 07 ” февраля 2017 г.

РЕГЛАМЕНТ
Удостоверяющего Центра

Редакция № 4

Введен в действие Приказом № 3 от “ 07 ” февраля 2017 г.

Воронеж, 2017

1. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

1.1. Общие сведения

Общество с ограниченной ответственностью Телекоммуникационная компания «Контакт», именуемое в дельнейшем «Удостоверяющий Центр» (УЦ), зарегистрировано на территории Российской Федерации в городе Воронеж. Свидетельство о государственной регистрации юридического лица серия 36 № 002326624, выдано 28 июля 2005 года Межрайонной инспекцией Федеральной налоговой службы по крупнейшим налогоплательщикам по Воронежской области, Основной государственный регистрационный номер 1053600293977.

Удостоверяющий Центр в качестве профессионального участника рынка услуг по созданию и выдаче сертификатов ключей проверки электронных подписей осуществляет свою деятельность на территории Российской Федерации в соответствии с Федеральным законом от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи», а также следующих лицензий:

- Лицензия Управления ФСБ России по Воронежской области № 0006134 от 14 августа 2014 г. на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- Лицензия Федеральной службы по техническому и экспортному контролю серия КИ 0246 № 012374 от 26 декабря 2012 г. на деятельность по технической защите конфиденциальной информации;
- Лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций № 134447 от 12 декабря 2015 г. на телематические услуги связи.

1.2. Контактная информация

Наименование: Общество с ограниченной ответственностью Телекоммуникационная компания “Контакт” (ООО ТК “Контакт”)

Юридический адрес: 394000, г. Воронеж, ул. Пятницкого, д. 55.

Фактическое местонахождение: 394062, г. Воронеж, ул. Южно-Моравская, д. 2.

Банковские реквизиты (наименование банка, БИК, ИНН, р/с, к/с):

- Центрально-Черноземный банк ПАО Сбербанк г. Воронеж
- БИК 042007681
- ИНН 3666125216
- Р/с 40702810513000024235
- К/с 30101810600000000681

Контактные телефоны, факс, адрес электронной почты:

тел./факс (473) 260-65-67, 260-65-66; E-mail: mail@ktkt.ru, ca@ktkt.ru

Время работы: опубликовано на сайте УЦ по адресу http://uc.ktkt.ru.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Владелец сертификата ключа проверки электронной подписи
(Владелец сертификата ключа)

Лицо, которому в соответствии с законодательством Российской Федерации и настоящим Регламентом выдан сертификат ключа проверки электронной подписи.

Запрос на сертификат

Сообщение, содержащее необходимую информацию для получения сертификата.

Запрос на прекращение действия сертификата

Сообщение, содержащее необходимую информацию для прекращения действия сертификата.

Ключ проверки электронной подписи

Криптографический ключ, который связан с ключом электронной подписи с помощью особого математического соотношения. Ключ проверки электронной подписи известен другим пользователям системы и предназначен для проверки электронной подписи и шифрования. При этом ключ проверки электронной подписи не позволяет вычислить ключ электронной подписи.

Ключ электронной подписи

Криптографический ключ, который хранится пользователем системы в тайне. Используется для формирования электронной подписи и/или шифрования данных.

Ключ электронной подписи Удостоверяющего Центра

Ключ электронной подписи, использующийся Удостоверяющим Центром для создания сертификатов ключей и списков отозванных сертификатов.

Ключевой носитель

Носитель информации, содержащий один или несколько ключей.

Компрометация ключа

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Криптографический ключ (Ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Плановая смена ключей

Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Пользователи сертификатов ключей

Лица, использующие для каких-либо целей сертификаты ключей, созданные Удостоверяющим Центром.

Реестр сертификатов

Реестр выданных и аннулированных Удостоверяющим Центром сертификатов ключей, включающий в себя информацию, содержащуюся в выданных Удостоверяющим Центром сертификатах ключей, и информацию о датах прекращения действия или аннулирования сертификатов ключей, а также об основаниях такого прекращения и аннулирования.

Сертификат ключа проверки электронной подписи (Сертификат ключа)

Электронный документ, выданный Удостоверяющим Центром либо доверенным лицом Удостоверяющего Центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат ключа Удостоверяющего Центра

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

Служба актуальных статусов сертификатов

Сервис Удостоверяющего Центра (построенный на базе протокола OCSP), с использованием которого подписываются электронной подписью и предоставляются электронные ответы, содержащие информацию о статусе сертификатов ключей, выданных Удостоверяющим Центром.

Служба штампов времени

Сервис Удостоверяющего Центра (построенный на базе протокола TSP), с использованием которого подписываются электронной подписью и предоставляются штампы времени.

Список отозванных сертификатов

Электронный документ, подписанный электронной подписью Удостоверяющего Центра, формируемый на определенный момент времени и включающий в себя список серийных номеров сертификатов ключей, действие которых прекращено до окончания срока их действия или которые аннулированы.

Средство электронной подписи

Аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной подписи в электронном документе с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи в электронном документе, создание ключей электронной подписи и ключей проверки электронной подписи.

Штамп времени электронного документа (Штамп времени)

Электронный документ, подписанный электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

Cryptographic Message Syntax (CMS)

Стандарт, определяющий формат и синтаксис криптографических сообщений.

PKCS #10

Стандарт, определяющий формат и синтаксис запросов на сертификат по рекомендациям IETF RFC 2986 "PKCS #10: Certification Request Syntax Specification (2000)" и IETF RFC 4491 "Using GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile"

Online Certificate Status Protocol (OCSP)

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

Time-Stamp Protocol (TSP)

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

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Статус Регламента

Регламент оказания услуг Удостоверяющего Центра, именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

Регламент устанавливает общий порядок и условия предоставления Удостоверяющим Центром пользователю, присоединившемуся к Регламенту в порядке, предусмотренном статьёй 428 ГК РФ, услуг по созданию и выдаче сертификатов ключей и дополнительных услуг, связанных с управлением сертификатами ключей.

Любой пользователь может ознакомиться с Регламентом на сайте Удостоверяющего Центра (http://uc.ktkt.ru), либо в офисе Удостоверяющего Центра по адресу г. Воронеж, ул. Южно-Моравская, д. 2, и по запросу получить его копию.

3.2. Применение Регламента

Настоящий Регламент налагает обязательства на все вовлеченные стороны, а также служит средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

Применение Регламента основано на его добровольном признании взаимодействующими сторонами. Добровольное признание настоящего Регламента другой стороной является основанием заключения соглашения о взаимодействии и оказания услуг.

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

В случае противоречия и/или расхождения названия какой-либо статьи со смыслом какого-либо пункта в ней содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

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

3.3. Изменения Регламента

Внесение изменений в Регламент, включая приложения к нему, производится Удостоверяющим Центром в одностороннем порядке.

Уведомление о внесении изменений в Регламент осуществляется Удостоверяющим Центром путем публикации на сайте УЦ по адресу http://uc.ktkt.ru.

Изменения, вносимые Удостоверяющим Центром в Регламент, не связанные с изменением законодательства Российской Федерации, вступают в силу и становятся обязательными с даты их публикации на сайте УЦ по адресу http://uc.ktkt.ru.

Изменения, вносимые Удостоверяющим Центром в Регламент в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих нормативно-правовых актов.

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

Порядок внесения изменений и публикация приложений к настоящему Регламенту осуществляется в порядке, соответствующем порядку внесения изменений и публикации Регламента.

3.4. Услуги, предоставляемые Удостоверяющим Центром

В процессе своей деятельности Удостоверяющий Центр предоставляет следующие виды услуг:

1. создание сертификатов ключей в электронной форме;
2. изготовление копии сертификатов ключей на бумажном носителе по запросу;

3. создание ключей электронной подписи и ключей проверки электронной подписи по обращениям заявителей с записью их на ключевой носитель;
4. ведение реестра сертификатов ключей;
5. предоставление сертификатов ключей в электронной форме, находящихся в реестре выданных сертификатов по запросу;
6. прекращение действия сертификатов ключей:

- по истечении срока его действия;
- по обращениям владельцев сертификатов ключей;
- в иных случаях, установленных Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим Центром и владельцем сертификата ключа, а также настоящим Регламентом;

7. предоставление сведений из реестра сертификатов об аннулированных сертификатах ключей и сертификатах ключей, действие которых прекращено;
8. подтверждение подлинности электронных подписей в документах, представленных в электронной форме, в отношении выданных им сертификатов ключей по обращениям заявителей;
9. подтверждение подлинности электронных подписей Удостоверяющего Центра в созданных им сертификатах по обращениям заявителей;
10. иные услуги связанные с использованием электронных подписей.

3.5. Прекращение деятельности

Деятельность Удостоверяющего Центра может быть прекращена в порядке, установленном законодательством Российской Федерации.

В случае прекращения деятельности Удостоверяющего Центра реестр Удостоверяющего Центра, включающий реестр сертификатов, передаются в Уполномоченный федеральный орган.

3.6. Стоимость услуг

Удостоверяющий Центр осуществляет свою деятельность на платной основе.

Стоимость и состав услуг Удостоверяющего Центра определяются прейскурантом, опубликованным на сайте УЦ по адресу http://uc.ktkt.ru.

Сроки и порядок расчетов за услуги, оказываемые Удостоверяющим Центром, регулируются условиями договоров между Удостоверяющим Центром и заявителем.

Создание сертификатов ключей в случаях, вызванных внеплановой сменой ключей Удостоверяющего Центра, связанной с нарушением конфиденциальности ключей электронной подписи Удостоверяющего Центра (п. 9.7.2 настоящего Регламента), осуществляется Удостоверяющим Центром безвозмездно.

Удостоверяющий Центр в порядке, предусмотренном настоящим Регламентом, безвозмездно предоставляет сертификаты ключей в форме электронных документов из реестра выданных сертификатов Удостоверяющего Центра, а также безвозмездно публикует список отозванных сертификатов.

4. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

4.1. Предоставление информации и документов

1. Заявитель представляет в Удостоверяющий Центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности заявителя (доверенного лица заявителя), а также документы, на основании которых Удостоверяющим Центром вносятся сведения в сертификат, такие как: полное или сокращенное наименование, основной государственный регистрационный номер, адрес местонахождения, идентификационный номер налогоплательщика, код причины постановки на учет, страховой номер индивидуального лицевого счета, наименование должности и иные данные.
2. Если для подтверждения каких-либо сведений, вносимых в сертификат, действующим законодательством установлена определенная форма документа, заявитель представляет в Удостоверяющий Центр документ соответствующей формы;
3. К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами;
4. Предоставление документов для создания ключей и сертификата ключа, получения созданных Удостоверяющим Центром ключей и сертификата ключа, прекращения действия сертификата ключа может быть осуществлено:
   - для юридического лица:
     - физическим лицом, которое указывается в сертификате наряду с наименованием юридического лица;
     - физическим лицом на основании соответствующей доверенности, оформленной по форме опубликованной на сайте Удостоверяющего Центра (http://uc.ktkt.ru);
   - для физического лица:
     - непосредственно этим физическим лицом;
     - физическим лицом на основании соответствующей нотариально заверенной доверенности, оформленной по форме опубликованной на сайте Удостоверяющего Центра (http://uc.ktkt.ru).

4.2. Удостоверение личности

1. Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, Удостоверяющий Центр может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;
2. Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства, с учетом требований п. 4.1.3;
3. Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

5. ПРАВА

5.1. Права Удостоверяющего Центра

Удостоверяющий Центр имеет право:

1. Запросить у заявителя:
   - документы для подтверждения информации, содержащейся в заявлении на создание сертификата ключа;
   - документы, необходимые для разрешения противоречий между информацией, содержащейся в заявлении на создание сертификата ключа и в иных представленных документах;
   - документы, подтверждающие достоверность представленных им сведений при наличии противоречий между этими сведениями и сведениями, полученными Удостоверяющим Центром из государственных информационных ресурсов.
2. Производить проверку достоверности документов и сведений, представленных заявителем со сведениями, полученными из государственных информационных ресурсов.
3. Не принимать документы, не соответствующие требованиям действующих нормативно-правовых актов Российской Федерации и настоящего Регламента;
4. Отказать в создании сертификата ключа в случае ненадлежащего оформления заявления на создание сертификата ключа;
5. Отказать в создании сертификата ключа в случае не предоставления и/или ненадлежащего предоставления:
   - документов, необходимых для удостоверения личности заявителя или лица, выступающего от имени заявителя;
   - документов, подтверждающих право лица, выступающего от имени заявителя, обращаться за получением сертификата ключа;
   - документов, на основании которых Удостоверяющим Центром вносятся сведения в сертификат ключа, такие как: полное или сокращенное наименование, основной государственный регистрационный номер, адрес местонахождения (юридический адрес), идентификационный номер налогоплательщика, код причины постановки на учет, страховой номер индивидуального лицевого счета, наименование должности и иные данные.
6. Отказать в создании сертификата ключа в случае, если не было подтверждено, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа;
7. Отказать в создании сертификата ключа в случае, если использованное заявителем для формирования запроса на сертификат ключа средство электронной подписи не поддерживается Удостоверяющим Центром;
8. Отказать в прекращении действия сертификата ключа в случае ненадлежащего оформления соответствующего заявления на прекращение действия сертификата ключа, а также в случае, если сертификат ключа аннулирован или прекратил своё действие по другим основаниям;
9. Отказать в прекращении действия сертификата ключа в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификату ключа;
10. Без заявления владельца сертификата прекратить действие сертификата ключа в случае получения Удостоверяющим Центром достоверных сведений о компрометации ключа электронной подписи владельца сертификата ключа и/или невыполнения владельцем сертификата ключа обязанностей, установленных законодательством Российской Федерации в области электронной подписи;
11. Без заявления владельца сертификата прекратить действие сертификата ключ в случае получения Удостоверяющим Центром достоверных сведений о том, что документы, представленные заявителем для создания сертификата ключа,

не являются подлинными и/или не подтверждают достоверность всей информации, включенной в данный сертификат ключа;

12. Без заявления владельца сертификата прекратить действие сертификата ключа в случае невыполнения владельцем сертификата ключа обязанностей, определенных в п. 6.4 настоящего Регламента.

5.2. Права пользователей сертификатов ключей

Пользователи сертификатов ключей имеют следующие права:

1. Применять список отозванных сертификатов, изданный Удостоверяющим Центром, для установления статуса сертификатов ключей, созданных Удостоверяющим Центром;
2. Применять сертификат ключа Удостоверяющего Центра для проверки электронной подписи Удостоверяющего Центра в сертификатах ключей, созданных Удостоверяющим Центром;
3. Получить сертификат ключа, находящегося в реестре выданных сертификатов Удостоверяющего Центра;
4. Применять сертификат ключа для проверки электронной подписи электронного документа в соответствии со сведениями, указанными в сертификате ключа;
5. Пользоваться сервисами Службы актуальных статусов сертификатов и Службы штампов времени Удостоверяющего Центра;
6. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных подписей в документах, представленных в электронной форме;
7. Обратиться в Удостоверяющий Центр за подтверждением подлинности электронных подписей Удостоверяющего Центра в созданных им сертификатах ключей.

5.3. Права владельцев сертификатов ключей

Владельцы сертификатов ключей имеют права пользователей сертификатов ключей, а также дополнительно к ним следующие права:

1. Обратиться в Удостоверяющий Центр для прекращения действия сертификата ключа, владельцем которого они являются, в течение срока действия соответствующего ключа электронной подписи;
2. Обратиться в Удостоверяющий Центр на предмет получения (приобретения) средства электронной подписи.

6. ОБЯЗАННОСТИ

6.1. Обязанности Удостоверяющего Центра

6.1.1. Ключ электронной подписи Удостоверяющего Центра

Удостоверяющий Центр обязан:

1. Использовать для создания ключа электронной подписи Удостоверяющего Центра и формирования электронной подписи только сертифицированные в соответствии с действующим законодательством Российской Федерации средства электронной подписи;
2. Использовать ключ электронной подписи Удостоверяющего Центра только для подписи издаваемых им сертификатов ключей и списков отозванных сертификатов;
3. Принять меры по защите ключа электронной подписи Удостоверяющего Центра в соответствии с положениями настоящего Регламента.

6.1.2. Синхронизация времени

Удостоверяющий Центр организует свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Воронежа.

Удостоверяющий Центр обязан синхронизировать по времени все программные и технические средства обеспечения деятельности.

6.1.3. Создание ключей

Удостоверяющий Центр обязан:

1. Использовать для создания ключей электронной подписи заявителей только сертифицированные в соответствии с действующим законодательством Российской Федерации средства электронной подписи;
2. Обеспечить конфиденциальность созданных ключей электронной подписи;
3. Записать ключ на отчуждаемый носитель, в соответствии с требованиями по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей.

6.1.4. Создание сертификатов ключей

Удостоверяющий Центр обеспечивает создание сертификата ключа по обращению заявителя в соответствии с форматом и порядком, определенным в настоящем Регламенте.

Удостоверяющий Центр обязан:

1. Вносить в создаваемые сертификаты ключей только достоверную и актуальную информацию, подтвержденную соответствующими документами;
2. Обеспечить уникальность серийных номеров создаваемых сертификатов ключей;
3. Обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах ключей.

6.1.5. Прекращение действия сертификатов ключей

Удостоверяющий Центр обязан прекратить действие сертификата ключа по заявлению его владельца.

6.1.6. Уведомление

Удостоверяющий Центр обязан официально уведомить о прекращении действия или аннулировании сертификата ключа его владельца посредством публикации списка отозванных сертификатов.

6.1.7. Реестр сертификатов

Удостоверяющий Центр обязан вести реестр всех выданных и аннулированных Удостоверяющим Центром сертификатов ключей.

Удостоверяющий Центр обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

Реестр сертификатов ведется в электронном виде.

Сертификаты ключей представлены в реестре в форме электронных копий созданных сертификатов ключей.

Удостоверяющий Центр обязан публиковать выписки из реестра сертификатов, позволяющие определить действительность сертификатов ключей, изданных Удостоверяющим Центром.

Выписка из реестра сертификатов предоставляется в виде списка отозванных сертификатов в электронной форме и формате, определенном настоящим Регламентом.

Удостоверяющий Центр обязан обеспечивать круглосуточную доступность списка отозванных сертификатов в информационно-телекоммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания, составляющих не более 48 часов в месяц.

В случае проведения планового технического обслуживания Удостоверяющий Центр обязан уведомить пользователей сертификатов о возможных перебоях в работе, связанных с плановым техническим обслуживанием, не менее, чем за 2 (два) часа до начала такого обслуживания.

Уведомление о проведении технического обслуживания осуществляется путем публикации информации на сайте УЦ по адресу http://uc.ktkt.ru.

6.1.8. Публикация информации

Удостоверяющий Центр обязан публиковать актуальный список отозванных сертификатов на сайте Удостоверяющего Центра по адресу http://uc.ktkt.ru.

Период публикации списка отозванных сертификатов Удостоверяющего Центра – не более 12 часов.

6.1.9. Прочие обязанности

Удостоверяющий Центр обязан:

1. Осуществлять регистрацию квалифицированного сертификата ключа в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона № 63-ФЗ «Об электронной подписи»;
2. Осуществлять по желанию лица, которому выдан квалифицированный сертификат, безвозмездную регистрацию указанного лица в единой системе идентификации и аутентификации;
3. Уведомлять владельца сертификата ключа о фактах, которые стали известны Удостоверяющему Центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа.

6.2. Обязанности пользователей сертификатов ключей

Пользователь сертификата ключа, изданного Удостоверяющим Центром, обязан:

1. Перед использованием сертификата ключа удостовериться, что назначение сертификата ключа, определенное соответствующими областями использования, определенными в сертификате ключа согласно настоящему Регламенту, соответствует предполагаемому использованию.

6.3. Обязанности владельца сертификата ключа

Владелец сертификата ключа, изданного Удостоверяющим Центром, обязан:

1. Хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;
2. Применять для формирования электронной подписи только действующий ключ электронной подписи;
3. Не использовать ключ электронной подписи, при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4. Немедленно обратиться в Удостоверяющий Центр с заявлением на прекращение действия сертификата ключа в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи;
5. Не использовать ключ электронной подписи, связанный с сертификатом ключа, после подачи заявления на прекращение действия сертификата ключа в Удостоверяющий Центр до момента времени официального уведомления о прекращении действия сертификата ключа, либо об отказе в прекращении действия;
6. Не использовать ключ электронной подписи, связанный с сертификатом ключа, который аннулирован или действие которого прекращено;
7. Использовать ключ электронной подписи с учетом ограничений, содержащихся в соответствующем сертификате ключа;
8. Использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи средства электронной подписи, сертифицированные в соответствии с правилами сертификации Российской Федерации;
9. В случае самостоятельного создания ключа электронной подписи предоставить Удостоверяющему Центру запрос на сертификат в формате PKCS #10, с выполнением требований, предъявляемых к запросу на сертификат ключа Удостоверяющим Центром.

7. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

7.1. Типы конфиденциальной информации

Ключ электронной подписи владельца сертификата ключа является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа. Удостоверяющий Центр не осуществляет хранение ключей электронной подписи владельцев сертификатов ключей.

Персональная и корпоративная информация о владельцах сертификатов ключей, содержащаяся в Удостоверяющем Центре, не подлежащая непосредственной рассылке в качестве части сертификата ключа, списка отозванных сертификатов, считается конфиденциальной и не публикуется.

Информация, хранящаяся в журналах аудита Удостоверяющего Центра, считается конфиденциальной и не подлежит разглашению.

7.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией является открытой информацией.

Открытая информация может публиковаться по решению Удостоверяющего Центра. Место, способ и время публикации открытой информации определяется Удостоверяющим Центром.

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

Персональные данные, включаемые в сертификаты ключей, создаваемые Удостоверяющим Центром, относятся к общедоступным персональным данным.

Информация, содержащаяся в настоящем Регламенте, не является конфиденциальной.

7.3. Предоставление конфиденциальной информации

Удостоверяющий Центр имеет право раскрыть информацию, относящуюся к типу конфиденциальной информации, третьим лицам только в случаях требующих ее раскрытия в соответствии с действующим законодательством РФ или при наличии судебного постановления.

8. ПРОЦЕДУРЫ И МЕХАНИЗМЫ

8.1. Создание ключей и сертификатов ключей

Создание ключей электронной подписи осуществляется заявителем самостоятельно на своем рабочем месте или по обращению в Удостоверяющий Центр с использованием автоматизированного рабочего места Удостоверяющего Центра.

Создание сертификатов ключей осуществляется Удостоверяющим Центром по обращению физических лиц (в том числе - уполномоченных действовать от имени юридических лиц) и юридических лиц.

Обращение лиц оформляется в форме заявления на создание ключей и сертификатов ключей.

8.1.1. Создание и выдача ключей

Создание и выдача ключей в Удостоверяющем Центре осуществляется на основании заявления на создание ключей при личном прибытии заявителя в офис Удостоверяющего Центра.

Заявление на создание ключей подается заявителем лично в офис Удостоверяющего Центра по форме, опубликованной на сайте Удостоверяющего Центра (http://uc.ktkt.ru), на бумажном носителе и заверяется собственноручной подписью заявителя.

В случае, если заявитель не может прибыть лично в офис Удостоверяющего Центра, он должен выдать доверенному лицу, прибывающему в офис Удостоверяющего Центра для создания и получения ключей, доверенность на предоставление документов и получение ключей в соответствии с п. 4.1.4.

Заявление на создание ключей рассматривается ответственным сотрудником УЦ в течение 1 (одного) рабочего дня с момента поступления.

Создание ключей в Удостоверяющем Центре осуществляется на автоматизированном рабочем месте, аттестованном на соответствие требованиям по технической защите конфиденциальной информации, размещенном в аттестованном помещении Удостоверяющего Центра, доступ в которое ограничен.

Созданные ключи записываются на ключевой носитель, предоставляемый заявителем.

Предоставляемый заявителем ключевой носитель должен удовлетворять следующим требованиям:

- иметь тип устройства, входящий в перечень, определяемый Удостоверяющим Центром;
- быть проинициализированным (отформатированным);
- не содержать никакой информации, за исключением данных инициализации.

Ключевой носитель, содержащий созданные ключи, передается заявителю или доверенному лицу заявителя по окончании процедуры выдачи сертификата ключа. Факт выдачи ключей заносится в Журнал учета создания и выдачи ключей под роспись заявителя или доверенного лица.

8.1.2. Создание и выдача сертификата ключа

Создание и выдача сертификата ключа осуществляется Удостоверяющим Центром на основании заявления на создание сертификата ключа.

Заявление на создание сертификата ключа подается заявителем в Удостоверяющий Центр в электронном виде или на бумажном носителе по форме, опубликованной на сайте Удостоверяющего Центра (http://uc.ktkt.ru).

Заявление на создание сертификата ключа в электронном виде и запрос на сертификат ключа подаются в форме электронного документа формата CMS-сообщения, подписанного электронной подписью с использованием ключа электронной подписи и сертификата ключа, созданного Удостоверяющим Центром или квалифицированного сертификата ключа, созданного любым аккредитованным удостоверяющим центром, владельцем которых заявитель является.

Заявление на создание сертификата ключа на бумажном носителе подается заявителем лично в офис Удостоверяющего Центра и заверяется собственноручной подписью заявителя.

В случае, если заявитель не может прибыть лично в офис Удостоверяющего Центра, он должен выдать доверенному лицу, прибывающему в офис Удостоверяющего Центра для создания и получения сертификатов ключей, доверенность на предоставление документов и получение сертификатов ключей в соответствии с п. 4.1.4.

Срок рассмотрения заявления на создание сертификата ключа составляет 2 (два) рабочих дня с момента его поступления в Удостоверяющий Центр.

В случае создания сертификата ключа юридическому лицу, наряду с наименованием юридического лица в сертификат может вноситься информация о физическом лице, действующем от имени юридического лица на основании учредительных документов юридического лица или доверенности. Указанная доверенность должна быть действительной на момент создания сертификата ключа. Форма такой доверенности опубликована на сайте Удостоверяющего Центра (http://uc.ktkt.ru). Допускается не указывать в сертификате ключа физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат ключ используется для автоматического создания или автоматической проверки электронной подписи.

Сотрудник Удостоверяющего Центра, путем установления личности по паспорту или иному документу удостоверяющему личность, выполняет процедуру идентификации заявителя или доверенного лица заявителя.

После положительной идентификации заявителя или доверенного лица заявителя, сотрудник Удостоверяющего Центра принимает документы и передает их ответственному сотруднику Удостоверяющего Центра на рассмотрение.

В случае отказа в создании сертификата ключа заявление на создание сертификата ключа вместе с приложениями возвращается заявителю с отметкой ответственного сотрудника Удостоверяющего Центра.

При принятии положительного решения, ответственный сотрудник Удостоверяющего Центра выполняет действия по созданию сертификата ключа.

По окончании процедуры создания сертификата ключа, заявителю выдаются:

- ключи, записанные на ключевой носитель (если требуется);
- сертификат ключа в электронной форме, соответствующий ключу электронной подписи;
- копия сертификата ключа на бумажном носителе, по форме определенной настоящим Регламентом (если требуется).

Заявитель ознакамливается со сведениями, содержащимися в созданном сертификате ключа, подписывает и передает сотруднику Удостоверяющего Центра копию сертификата ключа на бумажном носителе, содержащую указанные сведения.

Указанные выше данные, передаваемые заявителю в электронной форме, записываются в виде файлов на отчуждаемый носитель, предоставляемый заявителем.

По необходимости (в случае его отсутствия) заявитель должен приобрести (получить) средство электронной подписи, распространяемое Удостоверяющим Центром.

8.2. Прекращение действия сертификата ключа

8.2.1. Основания для прекращения действия сертификата ключа

Сертификат ключа прекращает свое действие в следующих случаях:

- по истечении срока его действия;
- по заявлению владельца сертификата ключа;
- в случаях, установленных законодательством РФ или соглашением между Удостоверяющим Центром и владельцем сертификата ключа;
- если Удостоверяющему Центру стало известно, что документы, на основании которых оформлен сертификат ключа, прекратили действие, не являются подлинными или не подтверждают достоверность всей информации, включённой в сертификат ключа.

Удостоверяющий Центр признает сертификат ключа аннулированным, если:

- не подтверждено, что владелец сертификата ключа владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате ключа;
- установлено, что содержащийся в сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа;
- вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа содержит недостоверную информацию.

8.2.2. Прекращение действия сертификата ключа по истечению срока его действия

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

8.2.3. Прекращение действия сертификата ключа по заявлению владельца

Прекращение действия сертификата ключа, созданного Удостоверяющим Центром, осуществляется Удостоверяющим Центром на основании заявления на прекращение действия сертификата ключа.

Заявление на прекращение действия сертификата ключа подается владельцем сертификата ключа (далее - заявитель) в Удостоверяющий Центр в электронном виде или на бумажном носителе по форме, опубликованной на сайте Удостоверяющего Центра (http://uc.ktkt.ru).

Заявление на прекращение действия сертификата ключа в электронном виде подается в форме электронного документа в формате CMS-сообщения, подписанного электронной подписью с использованием ключа электронной подписи и сертификата ключа, созданного Удостоверяющим Центром, владельцем которых заявитель является.

Заявление на прекращение действия сертификата ключа на бумажном носителе подается заявителем лично в офис Удостоверяющего Центра и заверяется собственноручной подписью заявителя.

В случае, если заявитель не может прибыть лично в офис Удостоверяющего Центра, он должен выдать доверенному лицу, прибывающему в офис Удостоверяющего Центра для подачи заявления, доверенность на предоставление документов в соответствии с п. 4.1.4.

Срок рассмотрения заявления на прекращение действия сертификата ключа составляет 1 (один) рабочий день с момента его поступления в Удостоверяющий Центр.

В случае отказа в прекращении действия сертификата ключа Удостоверяющий Центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения Удостоверяющий Центр осуществляет прекращение действия сертификата ключа.

8.2.4. Прекращение действия сертификата ключа по иным основаниям

Прекращение действия сертификата ключа по иным основаниям, указанным в п. 8.2.1, осуществляется в соответствии с действующим законодательством Российской Федерации.

8.2.5. Уведомление

В случае прекращения действия или аннулирования сертификата ключа, за исключением случая прекращения действия сертификата ключа по истечению срока его действия, информация о сертификате ключа, действие которого прекращено или аннулированном сертификате ключа, вносится в список отозванных сертификатов в течение 12 (двенадцати) часов с момента наступления описанного события, о чем Удостоверяющий Центр официально уведомляет владельца и всех пользователей сертификата ключа.

Официальным уведомлением о факте прекращения действия или аннулирования сертификата ключа является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате ключа, действие которого прекращено или аннулированном сертификате ключа, и изданного не ранее времени наступления произошедшего случая.

Временем прекращения действия или аннулирования сертификата ключа признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

8.3. Процедура подтверждения подлинности электронной подписи в электронном документе

Подтверждение подлинности электронной подписи в электронном документе осуществляется Удостоверяющим Центром по обращению лиц (далее по тексту раздела – заявитель), на основании заявления на подтверждение подлинности электронной подписи в электронном документе (далее по тексту раздела – заявление) в простой письменной форме.

Заявление должно содержать информацию о дате и времени формирования электронной подписи в электронном документе. Бремя доказывания достоверности даты и времени формирования электронной подписи в электронном документе возлагается на заявителя.

Обязательным приложением к заявлению является переносной носитель (flash-диск, CD/DVD-диск и др.), содержащий следующие файлы:

- электронный документ в формате CMS-сообщения, к которому применена электронная подпись, и его электронную подпись;
- сертификат ключа в электронной форме, с использованием которого необходимо проверить подлинность электронной подписи в электронном документе;
- сертификат ключа Удостоверяющего Центра в электронной форме, являющегося издателем сертификата ключа, с использованием которого необходимо проверить подлинность электронной подписи в электронном документе;
- список отозванных сертификатов Удостоверяющего Центра, являющегося издателем сертификата ключа, с использованием которого необходимо проверить подлинность электронной подписи в электронном документе.

Срок рассмотрения заявления составляет 3 (три) рабочих дня с момента его поступления в Удостоверяющий Центр.

В случае отказа от подтверждения подлинности электронной подписи в электронном документе заявителю возвращается заявление с резолюцией ответственного сотрудника Удостоверяющего Центра.

В случае принятия положительного решения Удостоверяющий Центр проводит работы по подтверждению подлинности электронной подписи в электронном документе и составляет заключение Удостоверяющего Центра.

Заключение содержит:

- время, место и основание проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- объекты исследований и материалы по заявлению, представленные эксперту или комиссии экспертов для проведения проверки (экспертизы);
- содержание и результат проверки электронной подписи в электронном документе (принадлежности электронной подписи в электронном документе владельцу сертификата ключа и отсутствия искажений в подписанном данной электронной подписью электронном документе);
- иные сведения в соответствии с федеральным законом.

Заключение составляется в простой письменной форме в двух экземплярах, подписывается собственноручной подписью эксперта или членами комиссии экспертов и заверяется печатью Удостоверяющего Центра. Один экземпляр заключения предоставляется заявителю.

Экспертиза осуществляется с применением штатных программных средств, входящих в комплект программного обеспечения Удостоверяющего Центра.

8.4. Процедура подтверждения подлинности электронной подписи Удостоверяющего Центра в сертификате ключа

Подтверждение подлинности электронной подписи Удостоверяющего Центра в сертификате ключа осуществляется Удостоверяющим Центром по обращению лиц (далее по тексту раздела – заявитель), на основании заявления на подтверждение подлинности электронной подписи Удостоверяющего Центра в сертификате ключа (далее по тексту раздела – заявление) в простой письменной форме.

Обязательным приложением к заявлению является переносной носитель (flash-диск, CD/DVD-диск и др.), содержащий следующие файлы:

- сертификат ключа в электронной форме, подвергающийся процедуре проверки;
- сертификат ключа Удостоверяющего Центра в электронной форме, являющегося издателем сертификата ключа, подвергающегося процедуре проверки;
- список отозванных сертификатов Удостоверяющего Центра, являющегося издателем сертификата ключа, подвергающегося процедуре проверки.

Срок рассмотрения заявления составляет 5 (пять) рабочих дней с момента его поступления в Удостоверяющий Центр.

В случае отказа от подтверждения подлинности электронной подписи Удостоверяющего Центра в сертификате ключа заявителю возвращается заявление с резолюцией ответственного сотрудника Удостоверяющего Центра.

В случае принятия положительного решения Удостоверяющий Центр проводит работы по подтверждению подлинности электронной подписи Удостоверяющего Центра в сертификате ключа и составляет заключение Удостоверяющего Центра.

Заключение содержит:

- время, место и основание проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- объекты исследований и материалы по заявлению, представленные эксперту или комиссии экспертов для проведения проверки (экспертизы);
- содержание и результат проверки электронной подписи Удостоверяющего Центра в сертификате ключа (принадлежности электронной подписи в сертификате ключа Удостоверяющему Центру и отсутствия искажений в подписанном данной электронной подписью сертификате ключа);
- иные сведения в соответствии с федеральным законом.

Заключение составляется в простой письменной форме в двух экземплярах, подписывается собственноручной подписью эксперта или членами комиссии экспертов и заверяется печатью Удостоверяющего Центра. Один экземпляр заключения предоставляется заявителю.

Экспертиза осуществляется с применением штатных программных средств, входящих в комплект программного обеспечения Удостоверяющего Центра.

8.5. Процедура получения информации о статусе сертификата ключа

Получение информации о статусе сертификата ключа, созданного Удостоверяющим Центром, осуществляется по обращению лиц (далее по тексту раздела - заявитель), на основании заявления на получение информации о статусе сертификата (далее по тексту раздела - заявление) в простой письменной форме.

Заявление должно содержать следующую информацию:

- дата и время, на момент наступления которых требуется установить статус сертификата ключа;
- идентификационные данные владельца, статус сертификата ключа которого требуется установить;
- серийный номер сертификата ключа, статус которого требуется установить.

Срок рассмотрения заявления составляет 5 (пять) рабочих дней с момента его поступления в Удостоверяющий Центр.

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

8.6. Механизм доказательства обладания ключом электронной подписи, соответствующим ключу проверки электронной подписи

Заявления на создание сертификатов ключей, поступающие в Удостоверяющий Центр от владельцев ключей проверки электронной подписи, должны содержать собственноручную подпись (для заявлений на бумажном носителе) или электронную подпись (для заявлений в электронном виде) заявителя и в качестве реквизита запрос на сертификат, подготовленный в соответствии с форматом CMS-сообщений.

Подтверждение электронной подписи запроса на сертификат из заявления на создание сертификата ключа и наличие собственноручной подписи (для заявлений на бумажном носителе) или электронной подписи (для заявлений в электронном виде) заявителя подтверждает, что заявитель является владельцем ключа электронной подписи, соответствующему ключу проверки электронной подписи из заявления на создание сертификата ключа.

8.7. Предоставление сервисов Службы актуальных статусов сертификатов и Службы штампов времени

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

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

Адреса обращения к Службе актуальных статусов сертификатов Удостоверяющего Центра:

http://uc.ktkt.ru/ocsp2/ocsp.srf (для неквалифицированных сертификатов ключей);

http://uc.ktkt.ru/ocsp-g2/ocsp.srf (для квалифицированных сертификатов ключей).

Адрес обращения к Службе актуальных статусов сертификатов заносится в расширение Authority Information Access (AIA) создаваемых Удостоверяющим Центром сертификатов ключей.

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

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

Адрес обращения к Службе штампов времени Удостоверяющего Центра – http://uc.ktkt.ru/tsp/tsp.srf

9. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Сроки действия ключей и сертификатов ключей Удостоверяющего Центра

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

Начало периода действия ключа электронной подписи Удостоверяющего Центра исчисляется с даты и времени генерации ключа электронной подписи Удостоверяющего Центра.

Срок действия сертификата ключа Удостоверяющего Центра составляет не более 15 лет.

9.2. Сроки действия ключей Службы актуальных статусов сертификатов и Службы штампов времени

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

Начало периода действия ключа электронной подписи Службы актуальных статусов сертификатов и Службы штампов времени исчисляется с даты и времени начала действия соответствующего сертификата ключа.

Срок действия сертификата ключа Службы актуальных статусов сертификатов и Службы штампов времени составляет не более 15 лет.

9.3. Сроки действия ключей и сертификатов ключей

Максимальный срок действия ключа электронной подписи заявителя устанавливается эксплуатационной документацией применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи заявителя исчисляется с даты и времени начала действия соответствующего сертификата ключа. Время начала периода действия ключа электронной подписи и его окончания заносится в поля «notBefore» и «not After» поля «Private Key Validity Period» соответственно.

Срок действия сертификата ключа заявителя устанавливается Удостоверяющим Центром в момент его создания.

9.4. Срок хранения сертификата ключа

Хранение сертификата ключа, изданного Удостоверяющим Центром, в реестре сертификатов осуществляется в течение установленного срока действия сертификата ключа. По истечении указанного срока хранения сертификаты ключей переводятся в режим архивного хранения.

9.5. Сертификат ключа в электронной форме

Сертификат ключа в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую стандарту Международного союза телекоммуникаций ITU-T X.509 версии 3 и рекомендаций IETF (Internet Engineering Task Force) RFC 2459 и представленный в кодировке Base64.

9.6. Копия сертификата ключа на бумажном носителе

Копия сертификата ключа на бумажном носителе, представляет собой документ, содержащий следующие обязательные реквизиты:

- Серийный номер сертификата ключа;

- Идентификационные данные владельца сертификата ключа;
- Идентификационные данные издателя сертификата (идентификационные данные из сертификата ключа Удостоверяющего Центра);
- Сведения о средстве электронной подписи Удостоверяющего Центра;
- Сведения о ключе проверки электронной подписи владельца сертификата ключа и алгоритме его формирования;
- Сведения об областях использования ключа электронной подписи и сертификата ключа.

Копия сертификата ключа на бумажном носителе может содержать иные реквизиты по усмотрению Удостоверяющего Центра.

9.7. Смена ключей Удостоверяющего Центра

9.7.1. Плановая смена ключей Удостоверяющего Центра

Плановая смена ключей электронной подписи и соответствующего ему ключа проверки электронной подписи Удостоверяющего Центра выполняется в период действия ключа электронной подписи Удостоверяющего Центра.

Уведомление о проведении плановой смены ключей Удостоверяющего Центра осуществляется путем публикации информации на сайте УЦ по адресу http://uc.ktkt.ru.

Процедура плановой смены ключей Удостоверяющего Центра осуществляется в следующем порядке:

- Удостоверяющий Центр формирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Удостоверяющий Центр создает сертификат нового ключа проверки электронной подписи и подписывает его электронной подписью с использованием нового ключа электронной подписи;

Ранее действовавший ключ электронной подписи Удостоверяющего Центра используется в течение своего срока действия для формирования списков отозванных сертификатов в электронной форме, созданных Удостоверяющим Центром в период действия ранее действовавшего ключа электронной подписи Удостоверяющего Центра.

9.7.2. Внеплановая смена ключей Удостоверяющего Центра

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа электронной подписи Удостоверяющего Центра.

Уведомление о проведении внеплановой смены ключей Удостоверяющего Центра осуществляется путем рассылки соответствующего уведомления владельцам сертификатов ключей по электронной почте и/или публикации информации на сайте УЦ по адресу http://uc.ktkt.ru.

Все сертификаты ключей, подписанные с использованием ключа Удостоверяющего Центра, конфиденциальность которого нарушена, считаются прекратившими действие.

После прекращения действия сертификата ключа Удостоверяющего Центра выполняется процедура внеплановой смены ключей Удостоверяющего Центра. Процедура внеплановой смены ключей Удостоверяющего Центра выполняется в порядке, определенной процедурой плановой смены ключей Удостоверяющего Центра.

Все действовавшие на момент компрометации ключа электронной подписи Удостоверяющего Центра сертификаты ключей подлежат внеплановой смене.

10. СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ

10.1. Структура сертификата ключа, создаваемого Удостоверяющим Центром в электронной форме

Удостоверяющий Центр создает сертификаты ключей в электронной форме формата X.509 версии 3 (см. п. 9.4).

10.1.1. Базовые поля сертификата ключа

Сертификаты ключей содержат следующие базовые поля X.509:

Signature:	Электронная подпись Удостоверяющего Центра
Issuer:	Идентификационные данные Удостоверяющего Центра
Validity:	Даты начала и окончания срока действия сертификата
Subject:	Идентификационные данные владельца сертификата ключа
Subject Public Key Information:	Идентификатор алгоритма средства электронной подписи, с которыми используется данный ключ проверки электронной подписи, значение ключа проверки электронной подписи
Version:	Версия сертификата формата X.509 - версия 3
Serial Number:	Уникальный серийный номер сертификата в реестре сертификатов Удостоверяющего Центра

10.1.2. Расширения сертификата

Сертификаты ключей содержат следующие расширения:

Authority Key Identifier	Идентификатор ключа Удостоверяющего Центра
Subject Key Identifier	Идентификатор ключа владельца сертификата ключа
Key Usage	Назначение ключа
Extended Key Usage	Набор областей использования ключа (объектных идентификаторов), устанавливающих ограничения на применение электронной подписи совместно с сертификатом ключа (если такие ограничения установлены)
CRL Distribution Point	Точка распространения списка отозванных сертификатов, созданных Удостоверяющим Центром
Authority Information Access	Адрес размещения сертификата Удостоверяющего Центра, Адрес обращения к Службе актуальных статусов сертификатов
Private Key Validity Period	Срок действия ключа электронной подписи, соответствующего сертификату ключа

Квалифицированные сертификаты ключей дополнительно содержат следующие расширения:

Certificate Policies	Политики сертификата
Subject Sign Tool	Средство электронной подписи владельца

Issuer Sign Tool	Средства электронной подписи и УЦ издателя

Сертификаты ключей могут содержать иные поля и расширения по усмотрению Удостоверяющего Центра.

10.1.3. Объектные идентификаторы алгоритма

Удостоверяющий Центр использует следующие идентификаторы алгоритмов средства электронной подписи:

ГОСТ Р 34.10-94	1.2.643.2.2.20	Алгоритм ключей проверки электронной подписи
ГОСТ Р 34.10-2001	1.2.643.2.2.19	Алгоритм ключей проверки электронной подписи
ГОСТ Р 34.10-2012	1.2.643.7.1.1.1.1	Алгоритм ключей проверки электронной подписи
ГОСТ Р 34.10-2012	1.2.643.7.1.1.1.2	Алгоритм ключей проверки электронной подписи
ГОСТ Р 34.10-94	1.2.643.2.2.4	Алгоритм подписи
ГОСТ Р 34.10-2001	1.2.643.2.2.3	Алгоритм подписи
ГОСТ Р 34.10-2012	1.2.643.7.1.1.3.2	Алгоритм подписи
ГОСТ Р 34.10-2012	1.2.643.7.1.1.3.3	Алгоритм подписи
Диффи-Хеллмана	1.2.643.2.2.99	Алгоритм на базе экспоненциальной функции
Диффи-Хеллмана	1.2.643.2.2.98	Алгоритм на базе эллиптической кривой
Диффи-Хеллмана	1.2.643.7.1.1.6.1	Алгоритм на базе эллиптической кривой
Диффи-Хеллмана	1.2.643.7.1.1.6.2	Алгоритм на базе эллиптической кривой
ГОСТ Р 34.11-94	1.2.643.2.2.9	Алгоритм хеширования
ГОСТ Р 34.11-2012	1.2.643.7.1.1.2.2	Алгоритм хеширования
ГОСТ Р 34.11-2012	1.2.643.7.1.1.2.3	Алгоритм хеширования
ГОСТ 28147-89	1.2.643.2.2.21	Алгоритм шифрования

10.1.4. Формы имени

В сертификате ключа поля идентификационных данных Удостоверяющего Центра и владельца сертификата ключа содержат атрибуты имени формата X.509.

10.1.5. Ограничения на имена

Обязательными атрибутами поля идентификационных данных Удостоверяющего Центра являются:

Common Name	Псевдоним
Organization	Наименование организации, являющейся владельцем Удостоверяющего Центра
Locality	Город
Country	RU

Email	Адрес электронной почты

Дополнительными обязательными атрибутами поля идентификационных данных квалифицированного сертификата Удостоверяющего Центра являются:

Street	Адрес местонахождения организации, являющейся владельцем Удостоверяющего Центра
State	Субъект Федерации, где зарегистрирована организация
INN	ИНН
OGRN	ОГРН

Обязательными атрибутами поля идентификационных данных владельца сертификата ключа, являющегося физическим лицом, являются:

Common Name	Фамилия, имя, отчество
Locality	Город
State	Субъект Федерации, где зарегистрирована организация
Country	RU
Email	Адрес электронной почты

Дополнительными обязательными атрибутами поля идентификационных данных квалифицированного сертификата владельца сертификата ключа, являющегося физическим лицом, являются:

Surname	Фамилия
Given Name	Имя, отчество
SNILS	СНИЛС
INN	ИНН физического лица

Обязательными атрибутами поля идентификационных данных владельца сертификата ключа, являющегося юридическим лицом и физическим лицом, действующим от имени юридического лица, являются:

Common Name	Фамилия, имя, отчество или Наименование организации, которую представляет владелец сертификата ключа
Title	Должность в организации, которую занимает владелец сертификата ключа
Organization	Наименование организации
Locality	Город
State	Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата ключа
Country	RU
Email	Адрес электронной почты

Дополнительными обязательными атрибутами поля идентификационных данных квалифицированного сертификата владельца сертификата ключа, являющегося

юридическим лицом и физическим лицом, действующим от имени юридического лица, являются:

Surname	Фамилия
Given Name	Имя, отчество
Street	Адрес местонахождения организации
OGRN	ОГРН
SNILS	СНИЛС
INN	ИНН организации

10.2. Структура списка отозванных сертификатов (СОС), издаваемого Удостоверяющим Центром в электронной форме

Удостоверяющий Центр издает списки отозванных сертификатов в электронной форме (далее по тексту раздела – СОС) формата X.509 версии 2.

10.2.1. Расширения СОС

Удостоверяющий Центр использует следующие расширения:

Authority Key Identifier	Идентификатор ключа Удостоверяющего Центра
Reason Code	Код причины прекращения действия сертификата ключа