



Общество с ограниченной ответственностью «АНК»
192029, Россия, г. Санкт-Петербург, ул. Бабушкина д.3 офисы 304(б), 312
тел./факс +7 (812) 326-55-16
internet: <http://www.ank-pki.ru> , e-mail: ank@ank-pki.ru

«УТВЕРЖДАЮ»

Генеральный директор ООО «АНК»

Карпов А.Г.

«03» апреля 2015 г.



УДОСТОВЕРЯЮЩИЙ ЦЕНТР
электронной подписи
Общества с ограниченной ответственностью «АНК»

РЕГЛАМЕНТ ПРЕДОСТАВЛЕНИЯ УСЛУГ

Версия 7.0

г. Санкт-Петербург
2015 г.

Термины и определения

Термины и определения даны в соответствии с положениями Федерального закона № 63-ФЗ от 6 апреля 2011 г. «Об электронной подписи».

Владелец сертификата ключа проверки электронной подписи

Лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи

Ключ электронной подписи

Уникальная последовательность символов, предназначенная для создания электронной подписи

Ключ проверки электронной подписи

Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи

Средства электронной подписи

Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи

Средства удостоверяющего центра

программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра

Удостоверяющий центр

юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи»

Электронная подпись

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

Электронный документ

Документ, в котором информация представлена в электронно-цифровой форме.

Принятые обозначения и сокращения

АРМ	Автоматизированное рабочее место
БД	База данных
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ОИД	Идентификатор объекта
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКП	Сертификат ключа проверки электронной подписи (Сертификат ключа подписи)
СКЗИ	Средство криптографической защиты информации
СОС (CRL)	Список отозванных сертификатов
СРС	Сервер реестра сертификатов
СЭП	Средства (средство) электронной подписи
СУЦ	Средства удостоверяющего центра
УЦ	Удостоверяющий центр
ФЗ	Федеральный закон
ЦР	Центр регистрации удостоверяющего центра
ЦС	Центр сертификации удостоверяющего центра
ЭП	Электронная подпись

1. Введение

1.1. Обзорная информация

Настоящий Регламент определяет правила, механизмы и условия предоставления и использования услуг УЦ АНК, включая обязанности, права и ответственность пользователей услуг УЦ (владельцев сертификатов ключей проверки ЭП), персонала УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, направленные на обеспечение безопасной работы УЦ и содержит описание процедур и действий, которые УЦ использует при изготовлении, выдаче и управлении сертификатами ключей проверки ЭП.

1.2. Идентификация Регламента

Наименование документа: «Регламент предоставления услуг Удостоверяющего Центра Общества с ограниченной ответственностью «АНК».

Дата: «03» апреля 2015 года.

1.3. Область применения Регламента

Настоящий Регламент предназначен служить средством официального уведомления и информирования получателей услуг УЦ во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

1.4. Утверждение и публикация Регламента

Настоящий Регламент составляется в письменной форме, утверждается и заверяется собственноручной подписью руководителя ООО «АНК».

Регламент публикуется

- путем размещения Регламента в электронной форме на ресурсе УЦ, доступном по адресу <http://ank-pki.ru/download/reglament2015.doc>;
- путем отправки Регламента (в электронной форме) с e-mail адреса УЦ ca@ank-pki.ru на адрес получателя (по запросам пользователей услуг УЦ);
- путем получения в УЦ АНК Регламента на бумажном носителе (по запросам пользователей услуг УЦ).

Электронная форма регламента подписана электронной подписью Уполномоченного лица УЦ.

1.5. Изменение Регламента

Удостоверяющий центр может вносить изменения и дополнения в текущую версию Регламента, а также принимать изменения в форме издания новых версий (редакций) Регламента. Изменению не подлежат положения Регламента, прямо или косвенно ущемляющие права пользователей услуг УЦ, за исключением случаев, когда такие изменения вносятся в соответствии с изменением законодательства Российской Федерации.

Утверждение изменений и дополнений, новых версий Регламента, их публикация осуществляется методами, предусмотренными в Регламенте.

1.6. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации. Нормы, содержащиеся в Регламенте, становятся обязательными для пользователей услуг УЦ с момента получения ими сертификата ключа проверки ЭП.

Срок действия Регламента – 1 год.

Если Удостоверяющий центр официально не уведомит пользователей услуг УЦ о прекращении действия Регламента, действие Регламента автоматически пролонгируется на следующий год.

Официальное уведомление о прекращении действия Регламента осуществляется методами, определенными в разделе «Публикация Регламента».

1.7. Ответственность

Удостоверяющий центр не несет ответственности в случае нарушения пользователями услуг УЦ положений настоящего Регламента.

Претензии к УЦ ограничиваются указанием на несоответствие его действий настоящему Регламенту.

2. Общие положения

2.1. Назначение Удостоверяющего центра АНК

Удостоверяющий центр предназначен для обеспечения участников (пользователей) различных систем электронного обмена данными и документами средствами ЭП, услугами и спецификациями для использования сертификатов ключей проверки ЭП в целях обеспечения:

- применения электронной подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия пользователей в электронных системах обмена данными и документами.

2.2. Услуги, предоставляемые Удостоверяющим центром АНК

В процессе своей деятельности УЦ предоставляет потребителям (пользователям) услуг УЦ следующие виды услуг:

- создает сертификаты ключей проверки ЭП и выдает такие сертификаты лицам, обратившимся за их получением (заявителям);
- устанавливает сроки действия сертификатов ключей проверки ЭП;
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки ЭП;
- выдает, по обращению заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП (созданные удостоверяющим центром или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП);

- ведет реестр выданных и аннулированных удостоверяющим центром сертификатов ключей проверки ЭП (далее - реестр сертификатов), включающий в себя:
 - информацию, содержащуюся в выданных удостоверяющим центром сертификатах ключей проверки ЭП,
 - информацию о датах прекращения действия или аннулирования сертификатов ключей проверки ЭП,
 - об основаниях прекращения или аннулирования;
- устанавливает
 - порядок ведения реестра сертификатов
 - порядок доступа к нему,
- обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов (с использованием информационно-телекоммуникационной сети «Интернет»);
- создает по обращениям заявителей ключи ЭП и ключи проверки ЭП;
- проверяет уникальность ключей проверки ЭП в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку ЭП;
- осуществляет иную связанную с использованием ЭП деятельность.

2.3. Пользователи услуг УЦ

Пользователями (получателями) услуг УЦ являются участники электронного взаимодействия, осуществляющие обмен информацией в электронной форме, к которому относятся:

- государственные органы,
- органы местного самоуправления,
- организации,
- граждане.

По отношению к составу предоставляемых услуг УЦ, пользователи услуг УЦ рассматриваются в настоящем Регламенте, как пользователи различных категорий:

- не имеющие собственных сертификатов, но использующие сертификаты других пользователей услуг УЦ (1-ая категория пользователей),
- зарегистрированные в УЦ и которым удостоверяющим центром выдан сертификат ключа проверки ЭП (2-ая категория пользователей, абоненты)

3. Права

3.1. Права Удостоверяющего центра АНК

Удостоверяющий центр имеет право:

- предоставлять сертификаты ключей проверки подписи в электронной форме, находящихся в реестре УЦ, всем лицам, обратившимся в Удостоверяющий центр;

- аннулировать (отозвать) сертификат ключа подписи пользователя УЦ в случае установленного факта компрометации ключа ЭП, с уведомлением владельца аннулированного (отозванного) сертификата и указанием обоснованных причин;

3.2. Права пользователей услуг УЦ

Пользователи 1-ой категории имеют следующие права:

- получить список аннулированных (отозванных) сертификатов ключей проверки подписи, изготовленный Удостоверяющим центром;
- получить сертификат ключа проверки подписи УЦ (Уполномоченного лица УЦ);
- получить сертификат ключа проверки подписи в электронной форме, находящегося в Реестре сертификатов Удостоверяющего центра;
- применять сертификат ключа проверки подписи Уполномоченного лица УЦ проверки ЭП подписи УЦ в сертификатах, изготовленных Удостоверяющим центром.
- применять сертификат ключа проверки подписи для проверки ЭП в соответствии со сведениями, указанными в сертификате.
- применять список аннулированных (отозванных) сертификатов ключей проверки подписи, изготовленный Удостоверяющим центром, для проверки статуса сертификатов ключей проверки подписи.
- обратиться в Удостоверяющий центр для предоставления (создания и выдачи) им ключей ЭП с записью их на ключевой носитель;
- обратиться в Удостоверяющий центр для внесения в реестр Удостоверяющего центра регистрационной информации о пользователе, с целью в дальнейшем стать владельцем сертификата ключа проверки подписи;
- обратиться в Удостоверяющий центр за подтверждением подлинности ЭП в документах, представленных в электронной форме;
- обратиться в Удостоверяющий центр за подтверждением подлинности ЭП Уполномоченного лица УЦ в изготовленном им сертификате;
- обратиться в Удостоверяющий центр на предмет получения (приобретения) средства электронной подписи;
- не принимать к исполнению электронные документы, подписанные ЭП, если:
 - сертификат ключа проверки ЭП отправителя не действует (находится в СОС) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
 - не подтверждена подлинность ЭП в электронном документе;
 - ЭП используется не в соответствии со сведениями, указанными в сертификате ключа проверки ЭП.

Пользователи 2-ой категории имеют права пользователей категории 1 и дополнительно имеют права:

- применять ключи ЭП и сертификаты ключей проверки подписи, владельцами которых они являются, для формирования ЭП на электронных документах в соответствии со сведениями указанными в сертификатах;
- обратиться в Удостоверяющий центр для аннулирования (отзыва) сертификата ключа проверки подписи в течении срока действия соответствующего ключа ЭП;
- использовать средства электронной почты, для передачи (пересылки) в Удостоверяющий центр заявления в форме электронного документа на аннулирование (отзыв) сертификата, подписанное ЭП;
- воспользоваться предоставляемыми Удостоверяющим центром программными средствами, для получения сертификатов ключей проверки подписи в электронной форме из Реестра сертификатов ключей подписи Удостоверяющего центра.

4. Обязательства

4.1. Обязательства Удостоверяющего центра АНК

Обязательствами УЦ по отношению к пользователям услуг УЦ являются:

- 1) информирование (в письменной форме):
 - об условиях и о порядке использования ЭП и средств ЭП,
 - о рисках, связанных с использованием ЭП,
 - о мерах, необходимых для обеспечения безопасности ЭП и их проверки
- 2) обеспечение актуальности информации, содержащейся в реестре сертификатов.
- 3) обеспечение защиты информации, содержащейся в реестре сертификатов от:
 - неправомерного доступа,
 - уничтожения,
 - модификации,
 - блокирования,
 - иных неправомерных действий.
- 4) предоставление любому лицу по его обращению (в соответствии с установленным порядком доступа к реестру сертификатов) информации, содержащейся в реестре сертификатов (в том числе информацию об аннулировании сертификата ключа проверки ЭП);
- 5) обеспечение конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.

Методами информирования являются:

- публикация настоящего Регламента и обеспечение свободного доступа к ознакомлению с его положениями;
- уведомление владельцев сертификатов о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа проверки ЭП;
- публикация информации, используемой для идентификации владельцев сертификатов ключей проверки ЭП, осуществляется путем включения ее в изготавливаемые сертификаты

Методом обеспечения актуальности является регулярная публикация информации об аннулировании сертификатов ключа проверки ЭП. Период публикации устанавливается в соответствии с условиями применения сертификатов в информационных системах, но не реже 1 раза в сутки. Удостоверяющий центр:

- ведет реестр сертификатов ключей проверки ЭП, обеспечивает его актуальность и возможность свободного доступа к нему пользователей услуг УЦ;
- вносит сертификаты ключей проверки ЭП в реестр выданных сертификатов ключей не позднее даты начала их действия и публикует реестр;
- предоставляет пользователям услуг УЦ доступ к реестру изготовленных сертификатов ключей проверки ЭП и списку отозванных сертификатов;
- обеспечивает выпуск и обновление списка отозванных и аннулированных сертификатов с указанием даты и времени аннулирования сертификата ключа проверки ЭП и причины аннулирования.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка отозванных сертификатов, содержащим сведения об аннулированном (отозванном) сертификате, на общедоступном веб-ресурсе УЦ (далее Репозитории).

Методом обеспечения защиты является применение комплексной системы защиты информации в автоматизированной системе, реализующей функции удостоверяющего центра. Удостоверяющий центр:

- создает ключи ЭП по обращению Заявителя с гарантией сохранения их в тайне;
- обеспечивает уникальность ключей ЭП;
- изготавливает сертификаты ключа проверки ЭП в форме документа на бумажном носителе и в форме электронного документа;
- размещает изготовленный ключ ЭП на отчуждаемый защищенный ключевой носитель пользователя услуг УЦ;
- обеспечивает уникальность регистрационной информации пользователей услуг УЦ, заносимой в реестр УЦ, используемой для идентификации владельцев сертификатов ключей проверки ЭП. УЦ не распространяет регистрационную информацию пользователей услуг УЦ, за исключением информации

используемой для идентификации владельцев сертификатов ключей проверки ЭП и заносимой в изготавливаемые сертификаты.

Удостоверяющий центр обеспечивает хранение сертификатов ключей ЭП в форме электронных документов после аннулирования не менее трех лет. По истечении указанного срока хранения, сертификаты ключей проверки ЭП исключаются из реестра сертификатов ключей ЭП и переводятся в режим архивного хранения. Сертификат ключа проверки ЭП в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

4.2. Обязательства пользователей услуг Удостоверяющего центра АНК

Лица, проходящие процедуру регистрации в УЦ, обязаны представить достоверную регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента.

Пользователи Удостоверяющего центра, в процессе работы с электронной подписью, подвергаются потенциальной возможности причинения вреда (риску), вследствие наступления следующих событий:

1) Для пользователей 2-й категории (владелец ключа электронной подписи):

– постороннее лицо сформировало электронную подпись от имени владельца сертификата ключа проверки электронной подписи. Это событие может наступить вследствие:

- 1) неосторожного обращения владельца сертификата ключа проверки электронной подписи с ключевым носителем, повлекшее утерю ключевого носителя и/или получение доступа посторонних лиц к ключу электронной подписи;
- 2) непреднамеренных действий посторонних лиц, вследствие которых последние получили доступ к ключу электронной подписи;
- 3) преднамеренных действий посторонних лиц, вследствие которых последние получили доступ к ключу электронной подписи;
- 4) формирования электронной подписи на подложном документе вследствие действия посторонних лиц в информационной системе, в которой применяется электронная подпись.

2) Для всех категорий пользователей УЦ

– лицо приняло к исполнению и/или к сведению электронный документ, удостоверенный электронной подписью, неверно идентифицировав лицо, сформировавшее электронную подпись, и/или его полномочия. Это событие может наступить вследствие:

- 1) недействительности сертификата ключа проверки электронной подписи;

- 2) несоответствия идентификационных данных владельца, записанных в сертификат ключа проверки электронной подписи, лицу, которое должно было подписать электронный документ;
 - 3) несоответствия вида документа и полномочий владельца сертификата ключа проверки электронной подписи, информация о которых приведена в сертификате ключа проверки электронной подписи или известна лицу, принимающему электронный документ к исполнению.
- лицо приняло к исполнению и/или к сведению искажённый электронный документ, удостоверенный электронной подписью. Это событие может наступить вследствие неосуществления проверки контроля целостности электронного документа и электронной подписи;

Для исключения возникновения вышеперечисленных рисков, владелец ключа ЭП и сертификата ключа проверки ЭП, выданного УЦ, обязан:

- хранить в тайне ключ ЭП, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;
 - не использовать для электронной подписи ключи ЭП, если ему известно, что эти ключи используются или использовались ранее другими лицами;
 - использовать ключ ЭП только для целей, разрешенных соответствующими областями использования, определенными в сертификате;
 - использовать сертификат ключа ЭП только для целей, разрешенных соответствующими областями использования, определенными в сертификате;
 - немедленно обратиться в УЦ с заявлением на аннулирование (отзыв) сертификата ключа проверки ЭП в случае, стало известно, что ключ ЭП используется или использовался ранее другими лицами;
 - соблюдать правила эксплуатации ключевого носителя
- 1) Ключевой носитель подключается через USB-порт компьютера и может выполнять свое функциональное назначение на вычислительных средствах, на которых установлено необходимое программное обеспечение.
 - 2) При получении ключевого носителя из УЦ, необходимо сменить PIN-код пользователя и пароль администратора;
 - 3) Пароль администратора необходимо держать в запечатанном конверте в труднодоступном месте;
 - 4) PIN-код пользователя должен быть известен только Владельцу сертификата;
 - 5) В процессе эксплуатации ключевого носителя Владелец сертификата не может удалять ключевой контейнер без согласования с администратором УЦ;

- б) Исключить возможность доступа к средству ЭП, несанкционированной модификации или его использования лицами, не имеющими допуска к работе со средством ЭП, а также исключить возможность использования ключей ЭП не уполномоченными на то лицами;

4.3. Разрешение споров

Сторонами в споре, в случае его возникновения, считаются УЦ и пользователь услуг УЦ.

При возникновении споров, стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, могут рассматриваться в суде в соответствии с действующим законодательством Российской Федерации.

5. Конфиденциальность информации

УЦ и пользователь услуг УЦ в процессе работы обязаны обеспечить сохранность конфиденциальной информации, полученной друг от друга в соответствии с действующим законодательством Российской Федерации.

Удостоверяющий центр обязан не разглашать (публиковать) информацию, полученную от Пользователя услуг УЦ, за исключением регистрационной информации включенной в изготовленные сертификаты ключа проверки ЭП.

Порядок предоставления конфиденциальной информации налоговым, правоохранительным и судебным органам осуществляется в соответствии с действующим законодательством Российской Федерации.

5.1. Типы конфиденциальной информации

Ключ ЭП владельца сертификата является конфиденциальной информацией данного пользователя УЦ. УЦ не депонирует и не архивирует ключи ЭП.

Персональная и корпоративная информация пользователей услуг УЦ, содержащаяся в УЦ, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки ЭП и списка отозванных сертификатов, считается конфиденциальной.

5.2. Типы информации, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной, считается открытой информацией. Открытая информация может публиковаться по решению Руководителя УЦ.

Место, способ и время публикации также определяется решением Руководителя УЦ. Информация, включаемая в сертификаты ключей проверки ЭП пользователей услуг УЦ и списки отозванных сертификатов, выдаваемые УЦ, не считается конфиденциальной.

5.3. Платность услуг

Услуги УЦ по созданию, управлению и обновлению сертификатов, а также услуги консультационного и информационно-справочного характера, оказываются на коммерческой основе по тарифам, установленным УЦ на момент их предоставления.

6. Средства предоставления услуг удостоверяющего центра АНК

В целях предоставления услуг и обеспечения жизнедеятельности УЦ использует автоматизированную систему (АС), реализующую целевые функции удостоверяющего центра и используемую для обеспечения заданного уровня безопасности обрабатываемой информации. В состав АС УЦ входят следующие функциональные компоненты:

- Центр Сертификации (ЦС);
- Центр Регистрации (ЦР);
- Автоматизированные рабочие места (АРМы) администратора и операторов ЦР;
- Автоматизированное рабочее место (АРМ) разбора конфликтных ситуаций.

Функционирование всех компонент АС УЦ обеспечено применением следующих технических средств:

- аппаратных платформ серверов, рабочих станций, средств организации информационного взаимодействия;
- программных комплексов операционных платформ;
- программного комплекса реализации целевых функций УЦ;
- средств защиты информации.

Центр Сертификации

Центр Сертификации (ЦС) является базовым серверным компонентом АС УЦ и предназначен для обеспечения реализации следующих целевых функций УЦ:

- формирование сертификатов ключей проверки ЭП пользователей УЦ в электронной форме с использованием ключа ЭП и сертификата ключа проверки ЭП Уполномоченного лица УЦ;
- формирование списков аннулированных сертификатов пользователей услуг УЦ;
- ведение Реестра сертификатов ключей проверки ЭП пользователей услуг УЦ;
- ведение списка аннулированных сертификатов ключей проверки ЭП пользователей услуг УЦ.

Центр Регистрации

Центр Регистрации (ЦР) является серверным компонентом АС УЦ и предназначен для обеспечения реализации следующих целевых функций УЦ:

- ведение Реестра зарегистрированных пользователей УЦ;
- ведение Реестра сертификатов;

- ведение Реестра заявлений на прекращение действия сертификатов пользователей услуг УЦ в электронной форме

АРМ администратора ЦР

АРМ администратора ЦР (АРМ ЦР) предназначен для управления ПК УЦ.

АРМ разбора конфликтных ситуаций

АРМ разбора конфликтных ситуаций (АРМ РКС) предназначен для разрешения вопросов, связанных с подтверждением электронной подписи Уполномоченного лица УЦ в сертификатах созданных УЦ.

6.1. Аппаратные средства УЦ

Аппаратные средства УЦ включают:

- выделенный сервер Центра Сертификации;
- выделенный сервер Центра Регистрации;
- телекоммуникационное оборудование;
- компьютеры рабочих мест персонала УЦ;
- устройства печати на бумажных носителях.

6.2. Энергоснабжение аппаратных средств УЦ

Электрические сети и электрооборудование, используемые в УЦ, отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Серверы Центра Сертификации и Центра Регистрации, рабочие станции персонала УЦ, телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течение 2 часов после прекращения основного электроснабжения.

6.3. Программные комплексы операционных платформ

В качестве программных комплексов операционных платформ компонент АС УЦ применяются операционные системы семейства Windows производства корпорации Microsoft.

6.4. Программный комплекс реализации целевых функций УЦ

В качестве программного комплекса реализации целевых функций используются:

- средства электронной подписи
- средства удостоверяющего центра

производства компании «КриптоПро».

6.4.1. Применяемые средства электронной подписи

Средства ЭП, применяемые Удостоверяющим центром и пользователями услуг УЦ для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи.

Применяемые средства ЭП не нарушают конфиденциальность информации содержащейся в документе при его подписи (проверки) ЭП.

В случаях неавтоматического (с участием пользователя) выполнения процедур создания и проверки электронной подписи, применяемые средства ЭП позволяют:

- установить факт изменения подписанного электронного документа (при проверке ЭП);
- обеспечить невозможность вычисления ключа ЭП из электронной подписи или из ключа проверки ЭП;
- показывать информационное содержание
 - подписываемого электронного документа (при создании ЭП);
 - подписанного электронного документа (при проверке ЭП);
- подтверждать операцию создания ЭП документа (при создании ЭП);
- показывать результат создания ЭП документа (при создании ЭП);
- определять владельца ключа ЭП, с использованием которого подписан электронный документ (при проверке ЭП).

Применяемые средства ЭП поддерживают криптографический интерфейс Cryptographic Service Provider (CSP) и удовлетворяют «Требованиям к средствам электронной подписи» (Утвержденным приказом ФСБ России от 27 декабря 2011 г. №796) класса криптографической защиты КС2.

В состав применяемых средств ЭП входит средство криптографической защиты информации «КриптоПро CSP» (версий 3.6) реализующее:

- выполнение процедур формирования и проверки ЭП в соответствии с российскими стандартами ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001;
- обеспечения свойств конфиденциальности и целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS.

6.4.2. Применяемые средства удостоверяющего центра

Программные и аппаратные средства, используемые в УЦ АНК, для реализации функций удостоверяющего центра удовлетворяют «Требованиям к средствам удостоверяющего центра» (Утвержденным приказом ФСБ России от 27 декабря 2011 г. №796) класса криптографической защиты КС2.

В состав применяемых средств удостоверяющего центра входит программно-аппаратный комплекс (ПАК) «Удостоверяющий Центр «КриптоПро УЦ» (версии 1.5) реализующий:

- регистрацию пользователей услуг УЦ;
- создание ключей электронных подписей;
- изготовление сертификатов ключей проверки ЭП;
- прекращение действия, аннулирование сертификатов ключей проверки подписей;
- ведение реестра сертификатов, обеспечение его актуальности и возможности доступа к нему участников информационных систем;
- выдача сертификатов ключей подписей в форме документов на бумажных носителях.

ПАК «КриптоПро УЦ» обеспечивает:

- применение совместно СКЗИ «КриптоПро CSP» версии 3.6
- выполнение функций создания и проверки электронной подписи в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, выполнение функций шифрования и имитозащиты в соответствии с ГОСТ 28147-89 с использованием СКЗИ «КриптоПро CSP» версии 3.6;
- формирование сертификатов ключей проверки подписей в соответствии с рекомендациями x.509v3 согласно RFC 3280 и RFC 5280 с учётом RFC 4491, позволяющими с помощью криптографических методов централизованно заверять соответствие открытого ключа атрибутам конкретного пользователя;
- аутентификацию программных компонент ПАК и пользователя при обмене информацией между ними.

6.5. Средства защиты информации УЦ

В состав автоматизированной системы УЦ АНК входит комплексная система защиты обрабатываемой информации, включающая:

- подсистему управления доступом, обеспечивающую:
 - идентификацию и аутентификацию (проверку подлинности)
 - разграничение полномочий сотрудников Общества из состава эксплуатирующего персонала АС УЦ АНК, выполняющих действия в соответствии с ролями, указанными в Регламенте при доступе к защищаемым ресурсам УЦ (включая функциональные режимы обработки информации);
- подсистему регистрации и учета, обеспечивающую:
 - регистрацию событий, связанных с безопасностью обработки и реализации целевых функций в журналах компонент УЦ;
 - возможность просмотра, поиска и анализа зарегистрированных событий;

- учет носителей защищаемой информации (включая носители ключевой криптографической информации)
- подсистему контроля целостности, обеспечивающую:
 - целостность обрабатываемой информации, программных средств и замкнутость программной среды АС УЦ;
 - целостность аппаратных средств АС УЦ;
 - возможность восстановления средств защиты информации от несанкционированного доступа (СЗИ НСД);
 - возможность резервного копирования восстановления наборов данных (баз данных)
- криптографическую подсистему, обеспечивающую использование ключей ЭП и сертификатов ключей проверки ЭП в механизмах идентификации и аутентификации;
- подсистему межсетевое экранирования, обеспечивающую разграничение сетевого взаимодействия компонент АС УЦ и пользователей услуг УЦ;
- подсистему антивирусной защиты.

6.6. Доступ к средствам УЦ

Физический доступ к аппаратным средствам компонент УЦ ограничивается путем их размещения в специальных помещениях:

- серверы центра сертификации и центра регистрации размещены в помещении «серверной». Серверное помещение является внутренним помещением и не имеет окон, выходящих на внешний периметр здания,
- АРМы операторов центра регистрации размещается в помещении фронт-офиса УЦ.

Оба помещения оборудованы датчиками охранной сигнализации с выходом на пульт централизованного контроля, находящимся на посту службы охраны здания. Персонал УЦ, допущенный в помещения УЦ АНК распоряжением руководителя ЗАО «АНК», обеспечен персональными кодами вскрытия и постановки на охрану данных помещений. Двери помещений оборудованы механическими замками, ключи от которых могут быть получены только лицами, которым установлены права на вскрытие помещений. В нерабочее время помещения находятся под охраной системы контроля, ключи от помещений, сданные под роспись в журнале службы охраны, находятся на посту охраны.

Помещения УЦ оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с Санитарно-гигиеническими нормами и Строительными нормами и правилами, устанавливаемыми законодательством Российской Федерации.

Серверное помещение УЦ оборудовано системой пожарной сигнализации в соответствии с требованиями руководящего документа НПБ 201-96 «Пожарная охрана предприятий. Общие требования».

Посетители допускаются в помещения УЦ только в рабочее время в сопровождении сотрудника из числа персонала Удостоверяющего центра.

Защита технических средств УЦ от несанкционированного доступа (НСД) обеспечивается применением:

- программно-аппаратных комплексов типа «электронный замок», реализующих режим доверенной загрузки операционной системы,
- защитных механизмов операционной системы Windows, реализующих дискреционную модель разграничения доступа,
- программно-аппаратных комплексов межсетевого экранирования и криптомаршрутизации, реализующих
 - режим ограничения сетевого взаимодействия с компонентами УЦ путем фильтрации сетевого трафика по заданным сетевым адресам, портам и протоколам загрузки операционной системы,
 - защищенный канал сетевого взаимодействия с территориально удаленными компонентами УЦ (АРМ-ами оператора).
- программных комплексов антивирусной защиты

6.7. Данные подлежащие резервному копированию

При эксплуатации УЦ выполняется ежедневное резервное копирование данных УЦ:

- база данных Центра Сертификации УЦ в формате базы данных Службы сертификации Microsoft (Microsoft Certificate Authority), включая журнал выданных сертификатов и очередь запросов;
- база данных Центра Регистрации УЦ (информация о зарегистрированных пользователях, запросах к Центру Регистрации и Центру Сертификации, хранящаяся в формате базы Microsoft SQL на сервере Центра Регистрации);

7. Эксплуатация автоматизированной системы, реализующей функции УЦ АНК

7.1. Состав группы эксплуатации УЦ

В рамках организационной структуры, объединяющей персонал УЦ, выделяются сотрудники, обеспечивающие его функционирование и исполняющие следующие роли:

- уполномоченное лицо УЦ;
- администратор центра регистрации;
- оператор центра регистрации;
- администратор безопасности;
- системный администратор;

- администратор разбора конфликтных ситуаций.

Один сотрудник УЦ может выполнять обязанности нескольких вышеперечисленных ролей.

7.2. Уполномоченное лицо УЦ

Уполномоченное лицо УЦ, назначается для проверки соответствия данных, вносимых в сертификат, Заявлению на изготовление сертификата, а также для заверения собственноручной подписью сертификата ключа проверки ЭП на бумажном носителе.

Уполномоченное лицо УЦ отвечает:

- за организацию работы персонала, исполняющего роли группы эксплуатации УЦ;
- за соответствие услуг, предоставляемых УЦ, положениям Регламента;
- за эксплуатацию технических средств и общесистемного программного обеспечения компонентов УЦ;
- за организацию работы по формированию изменений и дополнений, новых версий Регламента, их принятие и публикацию.

7.3. Администратор центра регистрации УЦ

В обязанности исполнителя роли Администратора центра регистрации УЦ входит решение следующих задач:

- по регистрации пользователей в УЦ;
- по ведению реестра зарегистрированных пользователей услуг УЦ;
- по изготовлению и выдаче ключей и сертификатов ключей проверки подписи сотрудникам и компонентам УЦ, пользователям услуг УЦ (в электронной форме и на бумажном носителе);;
- по распространению средств ЭП;
- по аннулированию (отзыву) сертификатов ключей проверки ЭП;
- по предоставлению пользователям услуг УЦ сведений об аннулированных сертификатах ключей проверки ЭП;
- по формированию предложений в части внесения изменений и дополнений в Регламент

7.4. Оператор центра регистрации УЦ

В обязанности исполнителя роли Оператора ЦР входят:

- прием заявок на создание и управление сертификатами ключей проверки ЭП от заявителей;
- прием документов, состав которых определен Регламентом УЦ для идентификации и аутентификации личности заявителей, подтверждения прав на обладание ключом ЭП;
- выполнения действий по идентификации и аутентификации личности заявителей;

- регистрация пользователей, от которых поступили заявки на создание сертификата ключа проверки ЭП;
- генерация ключей (ключевой пары) для изготовления сертификата пользователя;
- размещение ключей и сертификатов на защищенный ключевой носитель;
- выдача пользователям ключевых носителей, содержащих ключи и сертификаты изготовленные Удостоверяющим центром.

7.5. Администратор безопасности УЦ

В обязанности исполнителя роли администратора безопасности УЦ АНК входят:

- выполнение мероприятий по аудиту функционирования программно-аппаратного комплекса УЦ на предмет обеспечения безопасности обрабатываемой информации;
- управление разграничением доступа к компонентам УЦ ;
- управление средствами информационной безопасности УЦ, средствами криптографической защиты информации, (средствами ЭП) в соответствии с Регламентом УЦ, нормативными документами;
- выполнение процедурных действий по резервному копированию/восстановлению компонентов УЦ;
- управление межсетевым экранированием УЦ.

7.6. Системный администратор УЦ

В обязанности системного администратора УЦ входят:

- участие в установке и настройке программно-аппаратного комплекса УЦ и средств сетевого взаимодействия;
- контроль корректного функционирования УЦ в целях поддержания программно-аппаратного комплекса УЦ в работоспособном состоянии;
- выполнение действий по восстановлению работоспособности компонент УЦ.

7.7. Администратор разбора конфликтных ситуаций УЦ

В обязанности администратора по разбору конфликтных ситуаций входят:

- разбор конфликтной ситуации;
- идентификация спорной ситуации;
- определение сертификата, необходимого для проверки ЭП издателя;
- проверка ЭП издателя сертификата;
- проверка действительности сертификатов на текущий момент времени, применявшихся в процедурах, связанных с применением ЭП приведших к возникновению спорной ситуации;
- проверка отсутствия данных сертификатов в списке отозванных сертификатов (COC, CRL);

- сохранение результатов проверки на дисковом носителе и печать на бумажный носитель;
- составление протокола разбора конфликтной ситуации и заключения на основе полученных результатов.

7.8. Квалификации сотрудников

Эксплуатация технических средств УЦ, осуществляется персоналом, квалификация которого определяется условиями:

- для руководящего состава:
 - высшее профессиональное образование в области информационных технологий (информационной безопасности);
- для сотрудников, исполняющего роли оператора УЦ, администратора УЦ, администратора безопасности УЦ, системного администратора УЦ, администратора разбора конфликтных ситуаций УЦ:
 - высшее (среднее) профессиональное образования с переподготовкой (повышением квалификации по вопросам использования электронной подписи).

Состав и порядок выполнения действий, предусмотренных для исполнения каждой роли, изложен в «Технологических инструкциях». «Технологические инструкции» разработаны для каждой роли пользователей, эксплуатирующих УЦ. Содержание действий, установленных ролевыми «Технологическими инструкциями» определено в технической документации производителя продукта, используемого в качестве средства УЦ

8. Процедуры УЦ АНК

Удостоверяющий центр осуществляет следующие процедурные действия в отношении пользователей услуг УЦ:

- Регистрация пользователей услуг УЦ;
- Создание и выдача сертификата ключа проверки ЭП пользователю услуг УЦ;
- Аннулирование (отзыв) сертификата ключа проверки ЭП пользователю услуг УЦ.

Выполнение Удостоверяющим центром процедурных действий в отношении пользователей услуг УЦ возможно при установлении договорных отношений:

- между УЦ и пользователем услуг УЦ;
- между УЦ и оператором корпоративной информационной системы, определяющим участников электронного взаимодействия, использующих сертификаты ключа проверки ЭП, выдаваемые УЦ.

8.1. Регистрация пользователей услуг УЦ АНК

Процедура регистрации предусмотрена для внесения в УЦ данных о пользователях услуг УЦ и осуществляется:

- при личном присутствии пользователя или его уполномоченного представителя в Удостоверяющем центре;
- без личного присутствия. На основании полученных от него документов доверенным способом, (только для информационных систем, политика безопасности, которых предусматривает возможность удаленной регистрации пользователя УЦ, или не противоречит такой процедуре).

Основанием для выполнения Удостоверяющим центром процедуры регистрации, является:

- получение от лица (заявителя), обратившегося в УЦ, Заявления на создание и выдачу сертификата ключа проверки ЭП,

при условии, что

- заявитель (или оператор информационной системы) установил договорные отношения с УЦ и оплатил услугу по созданию и выдаче сертификата ключа проверки ЭП;
- заявитель не был зарегистрирован в УЦ ранее;
- заявитель был зарегистрирован в УЦ ранее, но его регистрационные данные изменились с момента первичной (предыдущей) регистрации;
- Удостоверяющим центром
 - установлена личность заявителя (физического лица, обратившегося в УЦ);
 - получено подтверждение правомочий обращения в УЦ (от лица, выступающего от имени заявителя - юридического лица)

При подаче Заявления на создание и выдачу сертификата ключа проверки ЭП, заявитель (или его доверенное лицо) предоставляет в УЦ документы (заверенные копии документов), подтверждающие достоверность данных Заявления, включаемых в сертификат:

- для заявителя - физического лица:
 - документ, удостоверяющий личность заявителя;
 - для доверенного лица, документ, удостоверяющий личность доверенного лица, и доверенность на представление интересов заявителя в удостоверяющем центре;
 - страховое свидетельство государственного пенсионного страхования заявителя.
- для заявителя - юридического лица:
 - учредительные документы,
 - документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц,

- свидетельство о постановке на учет в налоговом органе юридического лица;
- документ, удостоверяющий личность заявителя;
- для доверенного лица, документ, удостоверяющий личность доверенного лица, и доверенность на представление интересов заявителя в удостоверяющем центре;
- страховое свидетельство государственного пенсионного страхования заявителя (может не включаться по требованию организатора информационной системы).

8.2. Создание и выдача сертификата ключа проверки ЭП пользователю услуг УЦ АНК

Процедура создания и выдачи сертификата предусмотрена для зарегистрированных пользователей услуг УЦ и предполагает

- личное присутствие пользователя или его уполномоченного представителя в Удостоверяющем центре;
- без личного присутствия, для информационных систем, регламент которых предусматривает возможность удаленного издания сертификата ключа проверки ЭП, или не противоречит таковой процедуре..

Основанием для выполнения Удостоверяющим центром процедуры создания и выдачи сертификата является:

- полученное от лица (заявителя), обратившегося в УЦ, Заявления на создание и выдачу сертификата ключа проверки ЭП

В Заявлении могут быть указаны:

- необходимость создания Удостоверяющим центром ключа ЭП,
- либо необходимость использования Удостоверяющим центром ключа ЭП и ключа проверки ЭП, созданных заявителем.
- ограничения использования сертификата (если такие ограничения устанавливаются оператором информационной системы, в которой предполагается применение создаваемого сертификата).

Сертификат создается с использованием средств Удостоверяющего центра АНК, состав которых указан в настоящем Регламенте.

Оператор ЦР выполняет действия:

- по инициализации ключевого носителя,
- генерации ключей ЭП с размещением их в защищенное хранилище ключевого носителя,
- формированию запроса на создание сертификата.

- В случае использования ключа ЭП и ключа проверки ЭП, создаваемых непосредственно самим заявителем (без личного присутствия в УЦ), УЦ выдает заявителю средство формирования ключей ЭП и создания запроса на создание сертификата. Сформированный заявителем запрос на создание сертификата направляется Оператору ЦР и далее передается Администратору ЦР, который осуществляет контроль данных запроса и проверку их соответствия Заявлению и предоставленным в УЦ документам.
- направление сформированного запроса на создание сертификата его в Центр сертификации УЦ.

Результатом обработки Центром сертификации УЦ запроса является созданный сертификат ключа проверки ЭП.

Формат и структура создаваемого сертификата указаны в настоящем Регламенте.

Удостоверяющий центр создает сертификат в формах электронного документа, печатного бланка (документа на бумажном носителе) предназначенных для выдачи заявителю:

- сертификат в форме электронного документа размещается на отчуждаемый носитель.
- В случае создания Удостоверяющим центром ключа ЭП, ключ ЭП и сертификат ключа проверки ЭП размещаются на защищенный ключевой носитель;
- В случае использования ключа ЭП и ключа проверки ЭП, создаваемых непосредственно самим заявителем (без личного присутствия в УЦ), сформированный сертификат передается заявителю для размещения на ключевой носитель
- сертификат в форме документа на бумажном носителе изготавливается в двух экземплярах (один – для хранения Удостоверяющим центром, второй, – для выдачи заявителю)

Созданный Удостоверяющим центром сертификат в форме документа на бумажном носителе заверяется подписью Уполномоченного лица и печатью УЦ.

Созданный Удостоверяющим центром сертификат выдается после ознакомления заявителя с информацией, содержащейся в сертификате. Факт ознакомления и получения сертификата подтверждается личной подписью заявителя двух экземпляров сертификата на бумажном носителе.

Заявителю, получившему созданный сертификат ключа проверки ЭП (владельцу сертификата) Удостоверяющим центром выдается:

- руководство по обеспечению безопасности использования ЭП и средств ЭП (в случае обеспечения пользователя услуг УЦ средствами ЭП);
- парольная фраза для связи с УЦ. Владелец сертификата обеспечивает конфиденциальность парольной фразы.

8.3. Прекращение действия сертификата ключа проверки ЭП

Процедура прекращения действия сертификата предусмотрена для сертификатов выданных пользователям услуг УЦ и выполняется:

- в связи с истечением срока действия, установленного при его создании Удостоверяющим центром;
- на основании заявления владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности УЦ (без передачи его функций другим лицам);
- по решению суда, вступившему в законную силу, установившему, что сертификат ключа проверки ЭП содержит недостоверную информацию;
- не выполнением пользователем УЦ гарантийных обязательств в отношении УЦ;
- в иных случаях, которые могут быть установлены соглашением (договором) между УЦ и пользователем услуг УЦ.

Заявление владельца сертификата на прекращение его действия может быть подано:

- в форме документа на бумажном носителе
- или в форме электронного документа, содержащего действительную электронную подпись владельца.

Заявление включает в себя следующие обязательные сведения:

- идентификационные данные;
- серийный номер отзываемого сертификата;
- причину аннулирования (отзыва) сертификата.

При получении Заявления владельца сертификата на прекращение его действия, а также в случаях необходимости прекращения действия сертификата по иным причинам, предусмотренным настоящим Регламентом, УЦ аннулирует сертификат ключа проверки ЭП путем внесения записи о его аннулировании в реестр сертификатов и публикации списка аннулированных (отозванных) сертификатов.

9. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП

Срок действия ключа ЭП пользователя услуг УЦ, соответствующего сертификату ключа проверки подписи, владельцем которого он является, составляет 1 год.

Начало периода действия ключа ЭП пользователя услуг УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП пользователя услуг УЦ.

Срок действия ключа электронной подписи Уполномоченного лица УЦ составляет:

- 1 год, - для подписи сертификатов пользователей услуг УЦ;
- 3 года, - для подписи списка аннулированных (отозванных) сертификатов.

При плановой ежегодной смене сертификата ключа проверки подписи выполняется генерация ключевой пары (ключа ЭП, ключа проверки ЭП). УЦ обязуется осуществлять данную процедуру прозрачно для пользователей и без нарушения работоспособности системы.

10. Архивное хранение документированной информации

10.1. Состав архивируемых документов

Архивированию подлежат следующая документированная информация услуг УЦ:

- реестр сертификатов ключей проверки ЭП пользователей;
- сертификаты ключей проверки ЭП уполномоченного лица;
- журналы аудита программно-аппаратных средств обеспечения деятельности;
- реестр зарегистрированных пользователей;
- заявления на изготовление ключей подписи и сертификатов ключей проверки ЭП;
- заявления на прекращение действия, аннулирование (отзыв) сертификатов ключей проверки ЭП;
- служебные документы УЦ.

10.2. Архивохранилище

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

11. Формат сертификата ключа проверки ЭП, изготавливаемого УЦ АНК

Удостоверяющий центр изготавливает сертификаты ключей проверки ЭП пользователей услуг УЦ и уполномоченного лица УЦ в электронной форме:

- в формате спецификаций X.509 версии 3;
- в формате квалифицированного сертификата ключа проверки электронной подписи (утвержденном приказом ФСБ России от 27 декабря 2011 г. N 795).

Сертификат ключа проверки ЭП, создаваемый УЦ АНК содержит следующую информацию:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;

- фамилию, имя и отчество владельца сертификата (для физического лица) или наименование и место нахождения владельца сертификата (для юридического лица) или фамилия, имя и отчество лица, действующего от имени владельца сертификата - юридического лица на основании учредительных документов юридического лица или доверенности (уполномоченный представитель юридического лица);
- ключ проверки ЭП;
- наименование используемого средства ЭП и стандарты, требованиям которых соответствует ключ ЭП и ключ проверки ЭП;
- наименования средств ЭП и средств УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, сертификата, реквизиты документа, подтверждающего соответствие данных средств установленным требованиям;
- наименование и место нахождения УЦ, который выдал сертификат;
- номер сертификата УЦ;
- ограничения использования сертификата (если установлены).

Также сертификат может содержать дополнительную информацию о заявителе (соответствующую требованиям организатора информационной системы, в которой применяется сертификат):

- страховой номер индивидуального лицевого счета (СНИЛС) владельца сертификата (для физического лица) или уполномоченного представителя организации (для юридического лица);
- основной государственный регистрационный номер (ОГРН) владельца сертификата (для юридического лица);
- основной государственный регистрационный номер (ОГРНИП) владельца сертификата (для индивидуального предпринимателя);
- идентификационный номер налогоплательщика (ИНН) владельца сертификата (для юридического лица).

11.1. Базовые поля сертификата ключа проверки ЭП

Сертификаты ключей проверки ЭП содержат следующие базовые поля X.509:

algorithmidentifier	Идентификатор криптографического алгоритма, с использованием которого УЦ сформировал ЭП настоящего сертификата.
encrypted	ЭП, сформированная УЦ под структурированной совокупностью полей сертификата
version	Версия сертификата формата X.509 - версия 3 (значение 2)
serialnumber	Уникальный серийный (регистрационный) номер сертификата в реестре сертификатов ключей проверки ЭП УЦ

signature	Содержимое поля совпадает с содержимым поля algorithmIdentifier
issuer	Идентифицирующие данные УЦ (уполномоченного лица УЦ)
validity	Даты начала и окончания срока действия сертификата
subject	Идентифицирующие данные владельца сертификата ключа проверки ЭП
subjectPublicKeyInfo	значение ключа проверки ЭП владельца сертификата, и также идентификатор криптографического алгоритма, с которым должен использоваться ключ

11.2. Дополнения сертификата

Сертификаты ключей проверки ЭП содержат следующие дополнения:

authorityKeyIdentifier	идентификатор ключа УЦ. В поле authorityCertSerialNumber номер сертификата УЦ (уполномоченного лица УЦ)
KeyUsage	область использования ключа проверки ЭП, содержащегося в поле subjectPublicKeyInfo сертификата
certificatePolicies	обозначение политик сертификации
subjectSignTool	наименования используемого владельцем сертификата средства ЭП
issuerSignTool	наименования средств ЭП и средств УЦ, реквизитов документа, подтверждающего соответствие указанных средств установленным требованиям
subjectKeyIdentifier	Идентификатор ключа владельца сертификата
ExtendedKeyUsage	Область (области) использования ключа, при которых электронный документ с электронной подписью будет иметь юридическое значение
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) сертификатов ключей проверки ЭП, созданных УЦ

11.2.1. Объектные идентификаторы алгоритма

Удостоверяющий центр использует следующие объектные идентификаторы (ОИД) алгоритмов средства электронной подписи, имеющего наименование «СКЗИ КриптоПро CSP»:

ГОСТ Р 34.10-94	1.2.643.2.2.20
Диффи-Хеллмана	1.2.643.2.2.99
ГОСТ Р 34.10-2001	1.2.643.2.2.19
Диффи-Хеллмана	1.2.643.2.2.98
ГОСТ Р 34.11-94	1.2.643.2.2.9
ГОСТ 28147-89	1.2.643.2.2.21

11.2.2. Формы имени

В сертификате ключа проверки ЭП поля идентификационных данных уполномоченного лица УЦ и владельца сертификата содержат атрибуты имени формата X.500.

Основными атрибутами поля идентификационных данных являются:

common name*	имя, фамилия и отчество (для физического лица) наименование (для юридического лица). 2.5.4.3
Surname	фамилия физического лица. 2.5.4.4
givenName	имя и отчество (если имеется) физического лица. 2.5.4.42
countryName	двухсимвольный код страны (RU) 2.5.4.6
stateOrProvinceName*	наименование соответствующего субъекта Российской Федерации. 2.5.4.8
localityName	наименование населенного пункта. 2.5.4.7
streetAddress	часть адреса места нахождения, включающая наименование улицы, номер дома, корпуса, строения, квартиры, помещения (если имеется) 2.5.4.9
organizationName	наименование юридического лица 2.5.4.10
organizationUnitName	наименование подразделения юридического лица. 2.5.4.11
Title	наименование должности лица. 2.5.4.12
OGRN	строка, состоящая из 13 цифр представляющая ОГРН владельца сертификата (юридического лица). 1.2.643.100.1
OGRNIP	Строка, состоящая из 15 цифр представляющая ОГРНИП (только для ИП) 1.2.643.100.5
SNILS	строка, состоящая из 11 цифр представляющая СНИЛС владельца сертификата (физического лица). 1.2.643.100.3
INN	строка, состоящая из 12 цифр представляющая ИНН владельца сертификата. 1.2.643.3.131.1.1
email	Адрес электронной почты владельца сертификата 1.2.840.113549.1.9.1
Unstructured name	Строка может содержать дополнительные сведения о владельце сертификата 1.2.840.113549.1.9.2

Атрибуты поля, отмеченные *, являются обязательными для всех СКПЭП. Наличие остальных или дополнительных атрибутов (не приведенных в данной таблице), могут быть введены Регламентом информационной системы, в которой используется СКПЭП.

Данные Репозитория УЦ, в целях обеспечения гарантированного доступа со стороны пользователей услуг УЦ, дублируются на сетевых ресурсах («зеркала»), территориально размещаемых на объектах, обслуживаемых различными сервис-провайдерами.

12. График работы Удостоверяющего центра АНК

Услуги УЦ используемые для проверки ЭП предоставляются круглосуточно, семь дней в неделю, 365 дней в году.

Услуги УЦ в части приема заявлений в бумажной форме и изготовления сертификатов предоставляются с 9.00 до 18.00 по московскому времени в будние дни. Выходными днями являются: суббота, воскресенье, а также общегосударственные праздничные дни.

