МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный университет»

П Р И К А З

03.03.2021 №227/п

ОБ УТВЕРЖДЕНИИ РЕГЛАМЕНТА
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АлтГУ

В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»,

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемый Регламент удостоверяющего центра ФГБОУ ВО «Алтайский государственный университет».
2. Опубликовать Регламент удостоверяющего центра ФГБОУ ВО «Алтайский государственный университет» на сайте удостоверяющего центра ФГБОУ ВО «Алтайский государственный университет» uc.asu.ru.
3. Признать утратившим силу приказ ФГБОУ ВО «Алтайский государственный университет» от 18.09.2019 №1037/п «Об утверждении регламента удостоверяющего центра».

Ректор С.Н. Бочаров

Первый проректор по УР Е.А. Жданова

Начальник УПО В.В. Назаров

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Алтайский государственный университет»

УТВЕРЖДАЮ:
Ректор _____ С.Н.Бочаров
03 марта 2021 г.

Регламент удостоверяющего центра ФГБОУ ВО «Алтайский государственный университет»

г. Барнаул, 2021 г.

Термины и определения, используемые в настоящем Регламенте

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.
Квалифицированный сертификат ключа проверки электронной подписи	Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом "Об электронной подписи" от 06.04.2011 N 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;.
Средства 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, имеющие подтверждение соответствия требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
Список аннулированных сертификатов	Электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые были аннулированы до окончания срока их действия.
Удостоверяющий центр	Юридическое лицо или индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»
Ключ ЭП	Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.
Ключ проверки ЭП	Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
Средства ЭП	Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП
Заявитель	Коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной

	регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица (далее - нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата
Представитель УЦ	Сотрудник УЦ, обособленного подразделения УЦ, либо сотрудник третьего лица, ответственный за идентификацию лиц, обратившихся за получением квалифицированного СКПЭП, КЭП, проверку подлинности документов.

Список сокращений

СКЗИ	Средство криптографической защиты информации
СКПЭП, Сертификат	Сертификат ключа проверки электронной подписи
УЦ	Удостоверяющий центр
ЭП	Электронная подпись
КЭП	Квалифицированная электронная подпись
Владелец	Владелец квалифицированного сертификата ключа проверки электронной подписи
Регламент	Регламент Удостоверяющего центра ФГБОУ ВО «Алтайский государственный университет»
ПО	Программное обеспечение

1. Общие положения

1.1. Предмет регулирования Регламента.

1.1.1. Настоящий Регламент Удостоверяющего центра ФГБОУ ВО «Алтайский государственный университет», именуемый в дальнейшем - «Регламент», основан и учитывает положения действующего законодательства Российской Федерации, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», и устанавливает общий порядок и условия предоставления удостоверяющим центром услуг по изготовлению сертификатов ключей проверки электронной подписи и дополнительных услуг, связанных с управлением сертификатами ключей проверки электронной подписи.

1.1.2. Настоящий Регламент является договором присоединения на основании статьи 428 Гражданского кодекса РФ. Настоящий Регламент предназначен служить соглашением, налагающим обязанности по всем вовлечённым сторонам, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

1.1.3. Права и обязанности сторон по настоящему Регламенту, а также вопросы, не урегулированные настоящим документом, регламентируются действующим законодательством Российской Федерации и типовым Регламентом «КриптоПро УЦ»

1.1.4. Настоящий Регламент размещен для свободного доступа и ознакомления для всех заинтересованных лиц в электронной форме по адресу – uc.asu.ru

1.2. Сведения об Удостоверяющем центре.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Алтайский государственный университет», именуемое в дельнейшем «Удостоверяющий центр», «УЦ» зарегистрировано: Алтайский край, г. Барнаул, пр-т Ленина 61 (ОГРН 1022201770106, ИНН 2225004738 КПП 222501001, Свидетельство об аккредитации удостоверяющего центра рег. №858 от 28.03.2018 г.

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании лицензии, выданной Управлением Федеральной службы безопасности Российской Федерации по Алтайскому краю в соответствии с Постановлением Правительства Российской Федерации № 313 от 16 апреля 2012 года «Об утверждении Положения о лицензировании 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)».

Реквизиты ФГБОУ ВО «Алтайский государственный университет»:
Полное наименование: Федеральное государственное бюджетное образовательное учреждение высшего образования "Алтайский государственный университет"
ОГРН 1022201770106 **ИНН/КПП:** 2225004738/222501001
Юридический адрес: 656049, Алтайский край, г. Барнаул, пр. Л
Фактический адрес: 656049, Алтайский край, г. Барнаул, пр. Ленина, д. 61
Банковские реквизиты:
ОТДЕЛЕНИЕ БАРНАУЛ БАНКА РОССИИ//УФК по Алтайскому краю г. Барнаул БИК 010173001
Единый казначейский счет (вместо корр. счета): 40102810045370000009
Казначейский счет для осуществления и отражения операций с денежными средствами бюджетных учреждений (вместо расчетного счета): 03214643000000011700

График работы офиса: понедельник – пятница — с 08.00 до 17.00, суббота-воскресение — выходной. Обед: 12:00 – 12:48.

График работы технической поддержки: понедельник – пятница — с 08.00 до 17.00, суббота-воскресение — выходной. Обед: 12:00 – 12:48

1.3. **Порядок информирования о предоставлении услуг удостоверяющего центра.**
Контактные телефоны (факс) Удостоверяющего центра: **тел./факс (3852) 298-198;**
e-mail: uc@asu.ru
Электронный адрес: uc.asu.ru

Актуальная информация о телефонах, электронной почте Удостоверяющего центра размещена на официальном сайте УЦ ФГБОУ ВО «Алтайский государственный университет» по адресу: https://uc.asu.ru.

1.4. **Стоимость услуг Удостоверяющего центра.**

Информация о стоимости услуг Удостоверяющего центра указана на сайте удостоверяющего центра по адресу – uc.asu.ru/ (далее - Прайс).

Сроки и порядок расчётов за оказание услуг Удостоверяющего центра устанавливаются в соответствии с требованиями гражданского законодательства Российской Федерации. Оплата услуг может осуществляться, как путем полной предоплаты (аванса), путем частичной предоплаты, либо по факту оказания услуг.

Срок изготовления сертификата составляет не более 5 (пяти) рабочих дней с момента представления всех документов, необходимых для выпуска сертификата.

При оказании услуг по итогам проведения закупочных процедур, порядок и срок оказания услуг устанавливаются в соответствия с положениями заключенных контрактов.

В случае отказа заказчика от получения уже изготовленного на основании заявления сертификата, в случае предоплаты, уплаченные денежные средства не возвращаются.

1.5. Присоединение к Регламенту.

1.5.1. Фактом присоединения Заявителя к настоящему Регламенту является наиболее ранний из моментов:

а. предоставление Заявителем документов, необходимых для выпуска сертификата, в том числе заявления на изготовление сертификата ключа проверки электронной подписи;

б. оплата счета.

1.5.2. С момента выполнения одного из требований, указанных в пп. 1.5.1. Заявитель считается присоединившемся к Регламенту и является Стороной Регламента.

1.5.3. С момента присоединения Заявителя к настоящему Регламенту, Заявитель полностью и безоговорочно соглашается со всеми условиями настоящего Регламента и приложений к нему.

1.5.4. Заявитель, присоединившийся к настоящему Регламенту, самостоятельно отслеживает изменения (дополнения), вносимые в настоящий Регламент в виде его новой редакции, путем самостоятельного ознакомления с текстом Регламента на сайте Удостоверяющего центра по адресу – uc.asu.ru.

1.5.5. Заявитель самостоятельно отслеживает изменения в части применения и использования СКПЭП на сайте удостоверяющего центра по адресу – uc.asu.ru.

1.6. Изменение (дополнение) Регламента.

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

1.6.2. Уведомление Владельцев о внесении изменений (дополнений) в Регламент осуществляется удостоверяющим центром путем размещения очередной редакции настоящего Регламента, включающей указанные изменения (дополнения), на сайте удостоверяющего центра по адресу –uc.asu.ru.

1.7. Разрешение споров.

Сторонами в споре, в случае его возникновения, считаются УЦ и Заявитель.

Стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путём переговоров.

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

2. Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг)

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

2.1 Создание СКПЭП и выдача таких сертификатов лицам, обратившимся за их получением, при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получение данного сертификата;

2.2 Осуществление в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

2.3 Установление сроков действия СКПЭП;

2.4 Аннулирование выданных удостоверяющим центром СКПЭП;

2.5 Выдача по обращению Заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

2.6 Ведение реестра выданных и аннулированных Удостоверяющим центром сертификатов, в том числе включающего в себя информацию, содержащуюся в выданных этим Удостоверяющим центром сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов, а также об основаниях прекращения действия или аннулирования сертификатов;

2.7 Создание по обращениям Заявителей ключей электронных подписей и ключей проверки электронных подписей;

2.8 Проверка уникальности ключей проверки электронных подписей в Реестре сертификатов;

2.9 Проверка электронных подписей по обращениям участников электронного взаимодействия;

2.10 Осуществление иной деятельности, связанной с использованием электронной подписи.

3. Права и обязанности Удостоверяющего центра

3.1. Удостоверяющий центр обязан:

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

3.1.2. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.1.3. Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов.

3.1.4. Обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей.

3.1.5. Отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения СКПЭП.

3.1.6. Отказать заявителю в создании СКПЭП в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения СКПЭП.

3.1.7. При прекращении деятельности УЦ:

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

б. передать в уполномоченный федеральный орган в установленном порядке реестр выданных УЦ квалифицированных сертификатов;

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

3.1.7.1. При прекращении деятельности УЦ с переходом его функций другим лицам:

а. уведомить в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы УЦ и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций;

б. передать информацию, внесенную в реестр сертификатов, лицу, к которому перешли функции УЦ.

3.1.7.2. В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам уведомить в письменной форме владельцев СКПЭП, которые выданы этим УЦ и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности УЦ. В указанном случае после прекращения деятельности УЦ информация, внесенная в реестр сертификатов, будет уничтожена.

3.1.8. Вносить информацию о СКПЭП в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата.

3.1.9. Вносить информацию о прекращении действия СКПЭП в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие СКПЭП прекращается с момента внесения записи об этом в реестр сертификатов.

3.1.10. Уведомить владельца СКПЭП об аннулировании его СКПЭП путем направления электронного документа по электронной почте, указанной в заявлении на изготовление Сертификата до внесения в реестр сертификатов информации об аннулировании.

3.1.11. Хранить информацию, указанную в части 1 статьи 15 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», в течение срока деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, в форме, позволяющей проверить ее целостность и достоверность, а именно:

а. реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

б. сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

в. сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

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

3.1.13. Не использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

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

3.1.15. Соблюдать требования, на соответствие которым аккредитован, в течение всего срока аккредитации. В случае возникновения обстоятельств, делающих невозможным

соблюдение указанных требований, УЦ немедленно уведомляет об этом в письменной форме уполномоченный федеральный орган.

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

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

3.1.18. При выдаче квалифицированного СКПЭП иденифицировать заявителя - физического лица, обратившегося за получением квалифицированного СКПЭП.

3.1.19. Получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.

3.1.20. Ознакомить Заявителя с информацией, содержащейся в квалифицированном сертификате при выдаче квалифицированного СКПЭП.

3.1.21. Одновременно с выдачей квалифицированного сертификата предоставить владельцу СКПЭП руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи., об условиях и о порядке использования электронных подписей и средств электронной подписи (СКЗИ), о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей - Правила использования СКЗИ и ЭП (Приложение №1 к настоящему Регламенту).

3.1.22. Направлять в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.

3.1.23. По желанию владельца квалифицированного сертификата безвозмездно осуществлять его регистрацию в единой системе идентификации и аутентификации при выдаче квалифицированного сертификата с проведением идентификации владельца при его личном присутствии.

3.1.24. Вносить в СКПЭП только достоверную информацию, подтвержденную соответствующими документами.

3.1.25. На безвозмездной основе обеспечивать физических лиц шифровальными (криптографическими) средствами, указанными в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", для проведения идентификации физических лиц в аккредитованном удостоверяющем центре на основе предоставления биометрических персональных данных без личного присутствия посредством информационно-телекоммуникационной сети "Интернет"

3.2. Удостоверяющий центр имеет право:

3.2.1. Наделять третьих лиц полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению СКПЭП от имени УЦ.

3.2.2. Выдавать СКПЭП, как в форме электронных документов, так и в форме документов на бумажном носителе.

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

3.2.4. Отказать в изготовлении СКПЭП Заявителю в случае непредставления документов, предоставления документов не в полном объеме или предоставления документов, подлинность которых вызывает сомнение.

3.2.5. Отказать в изготовлении сертификата ключа подписи Заявителю в случае, если использованное Заявителем для формирования запроса на сертификат СКЗИ не поддерживается УЦ.

3.2.6. Отказать в изготовлении сертификата ключа подписи Заявителю в случае невыполнения Заявителем обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а так же Регламентом УЦ.

3.2.7. Отказать в изготовлении СКПЭП, если предоставленные Заявителем сведения не прошли проверку в соответствии с п.2.2, 2.3 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3.2.8. Отказать в изготовлении сертификата ключа подписи Заявителя подписи при расхождении данных, предоставленных Заявителем с данными, указанными в ЕГРЮЛ или ЕГРИП.

3.2.9. Без заявления владельца сертификата прекратить действие сертификата в случае наличия у Удостоверяющего центра достоверных сведений о нарушении конфиденциальности ключа электронной подписи владельца сертификата, а также невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи, а также в случае появления у Удостоверяющего центра достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность всей информации, включенной в данный сертификат, и/или в случае, если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке.

3.2.10. Проверять достоверность документов и сведений, предоставленных заявителем, с использованием инфраструктуры, запрашивать и получать из государственных информационных ресурсов:

а. выписку из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;

б. выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;

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

4. Права и обязанности Владельцев

4.1. Владелец обязан:

4.1.1. Обеспечить конфиденциальность ключа электронной подписи. Не использовать ключ электронной подписи и немедленно обратиться в аккредитованный удостоверяющий центр, выдавший сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.

4.1.2.Извещать Удостоверяющий центр обо всех изменениях данных, внесенных в сертификат.

4.1.3.При подаче заявления на СКПЭП указать действующий электронный почтовый адрес владельца СКПЭП для получения извещений, уведомлений от УЦ, связанных с применением СКПЭП, его аннулированием или прекращением.

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

4.1.5. Применять для формирования электронной цифровой подписи только действующий личный закрытый ключ.

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

4.1.7. Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате ключа подписи (расширения KeyUsage, Extended 2KeyUsage).

4.1.8. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия СКПЭП в случае утери, кражи, а также в случае если Владельцу стало известно, что ключ используется или использовался ранее другими лицами.

4.1.9. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на прекращение, действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата по момент времени официального уведомления об прекращение действия сертификата.

4.1.10. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который аннулирован.

4.2. Владелец имеет право:

4.2.1. Владелец, выданного в форме электронного документа, вправе получить также копию СКПЭП на бумажном носителе, заверенную УЦ.

4.2.2. Обратиться в УЦ с заявлением на изготовление СКПЭП.

4.2.3. Обратиться в УЦ с заявлением на аннулирование СКПЭП, владельцем которого он является, в течение срока действия соответствующего закрытого ключа.

4.2.4. Обратиться в УЦ за получением информации о статусе сертификатов ключей подписей и их действительности на определенный момент времени.

4.2.5. Обратиться в УЦ за подтверждением действительности электронной подписи в электронном документе, сформированной с использованием сертификата ключа подписи, изданного Удостоверяющим центром.

5. Порядок и сроки выполнения процедур, необходимых для предоставления услуг Удостоверяющим центром, в том числе требования к документам, предоставляемым в Удостоверяющий центр в рамках предоставления услуг

5.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей.

5.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей.

Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется одним из способов:

1) Создание Ключей электронной подписи и ключей проверки электронной подписи осуществляется в точке выдачи Удостоверяющего центра.

Ключ ЭП и соответствующий ему ключ проверки ЭП могут быть изготовлены в удостоверяющем центре на специализированном рабочем месте, аттестованном на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации, которое размещено в специально выделенном помещении.

2) Создание Ключей электронной подписи осуществляется Заявителем самостоятельно на своем рабочем месте, при этом Заявитель создает Ключ электронной подписи на своем рабочем месте с использованием предоставленных Удостоверяющим центром либо собственных Средств электронной подписи.

Ключ ЭП и ключ проверки ЭП, предназначенные для создания и проверки усиленной квалифицированной электронной подписи создаются с использованием средства ЭП, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Ключ электронной подписи и ключ проверки электронной подписи, независимо от способа создания, записывается на ключевой носитель.

5.1.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра, порядок информирования владельцев квалифицированных

сертификатов об осуществлении такой смены с указанием доверенного способа получения нового квалифицированного сертификата Удостоверяющего центра.

Плановая смена ключей ЭП УЦ выполняется в период действия ключа ЭП УЦ.

Плановая смена ключей ЭП производится по следующим основаниям:

а. истечение срока действия СКПЭП;

б. переход на использование новых стандартов ЭП и функции хэширования в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования электронной подписи.

Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

1) УЦ создает новый ключ ЭП и соответствующий ему ключ проверки ЭП;
2) УЦ изготавливает новый СКПЭП Уполномоченного лица УЦ.

При плановой замене ключа ЭП УЦ все Владельцы должны установить на своих компьютерах новый сертификат УЦ.

Информирование Заявителей/Владельцев о проведении плановой смены ключей уполномоченного лица удостоверяющего центра осуществляется посредством публикации информации на официальном сайте удостоверяющего центра по адресу: uc.asu.ru.

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте удостоверяющего центра по адресу: uc.asu.ru, доступная для скачивания.

Старый ключ ЭП УЦ используется в течение своего срока действия для формирования списков аннулированных сертификатов, изданных УЦ в период действия старого ключа ЭП УЦ.

5.1.3. **Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности.**

Внеплановая смена ключей выполняется в следующих случаях:

а. закрытый ключ УЦ закончил свой срок действия, а плановая смена произведена не была;

б. произошла компрометация закрытого ключа УЦ;

в. есть подозрение, что закрытый ключ УЦ мог быть скомпрометирован;

г. закрытый ключ УЦ не доступен (ключевой носитель поврежден, уничтожен и т.д.);

д. в связи с необходимостью внести изменение в содержимое сертификата УЦ (введение новых Требований к форме или формату сертификата и т.д.);

е. по решению, вступившему в законную силу (по решению суда, по решению владельца удостоверяющего центра и т.д.).

Актуальными угрозами нарушения конфиденциальности (компрометации) ключа электронной подписи Удостоверяющего центра являются:

- угрозы несанкционированного доступа, связанные с действиями нарушителей, имеющих доступ к рабочим местам автоматизированной системы удостоверяющего центра.

К случаям нарушения конфиденциальности (компрометации) ключа электронной подписи Удостоверяющего центра относятся в том числе:

а. физическая утеря/кража носителя ключа электронной подписи Удостоверяющего центра.

б. несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации или подозрение, что данные факты имели место (срабатывание сигнализации с подтверждением несанкционированного вскрытия помещения, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.)

в. иные случаи компрометации.

Процедура внеплановой смены ключей УЦ выполняется в порядке, определённом процедурой плановой смены ключей УЦ.

В случае компрометации ключа ЭП УЦ сертификат УЦ аннулируется, Владельцы уведомляются об указанном факте путем публикации информации о компрометации на сайте УЦ по адресу: uc.asu.ru.

Все сертификаты, подписанные с использованием скомпрометированного ключа УЦ, считаются аннулированными, с занесением соответствующих сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте удостоверяющего центра по адресу: uc.asu.ru, доступная для скачивания.

5.1.4. **Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца квалифицированного сертификата.**

5.1.4.1. Смена ключа ЭП владельца квалифицированного сертификата осуществляется в случаях:

а. истечения срока действия СКПЭП;

б. на основании заявления владельца СКПЭП о его аннулировании, подаваемого в форме документа на бумажном носителе или в форме электронного документа, и последующей подачей заявления на выпуск сертификата;

в. если не подтверждено, что владелец сертификата ключа проверки ЭП владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;

г. если установлено, что содержащийся в таком СКПЭП уже содержится в ином ранее созданном сертификате ключа проверки ЭП;

д. если вступило в силу решение суда, которым, в частности, установлено, что СКПЭП содержит недостоверную информацию;

е. иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и Владельцем.

5.1.4.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов.

При смене сертификата Владелец подает заявление на изготовление ключа проверки ЭП в соответствии с требованиями к заявлению, указанными в п. 5.2.2. настоящего Регламента.

5.1.4.3. При смене ключа ЭП владельца квалифицированного сертификата, заявление на изготовление СКПЭП может быть создано в форме электронного документа, подписанного усиленной квалифицированной подписью Владельца. При этом, в случае, если смена ключа электронной подписи владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, такое заявление должно быть подписано иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата.

5.1.4.4. Процедура выдачи квалифицированного сертификата и ключа электронной подписи владельца.

При выдаче квалифицированного сертификата УЦ:

а. идентифицирует заявителя - физическое лицо, обратившегося к нему за получением квалифицированного сертификата;

Идентификация гражданина Российской Федерации осуществляется:

1) при его личном присутствии по основному документу, удостоверяющему личность;

2) без его личного присутствия:

с использованием усиленной квалифицированной электронной подписи при наличии действующего квалифицированного сертификата;

путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные. Реализация

данного способа осуществляется с учетом требований постановления Правительства Российской Федерации от 8 ноября 2019 г. N 1427 "О проведении эксперимента по совершенствованию применения технологии электронной подписи";

путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства.

Идентификация беженца, вынужденного переселенца и лица без гражданства осуществляется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц;

б. получает от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата;

в. ознакамливает с информацией, содержащейся в СКПЭП;

Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица.

г. предоставляет владельцу СКПЭП руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств ЭП.;

д. направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.

е. безвозмездно осуществляет регистрацию владельца квалифицированного сертификата при его личном присутствии, в единой системе идентификации и аутентификации по его желанию.

ж) информирует заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

5.2. **Процедура создания и выдачи квалифицированных СКПЭП**.

5.2.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов.

5.2.1.1. Заявление может быть оформлено как на бумажном носителе, подписанное Заявителем собственноручно, так и в электронном виде, подписанное КЭП. Собственноручное подписание Заявления на бумажном носителе производится чернилами (пастой) синего или черного цвета.

5.2.1.2. Заявитель обращается с заявлением на изготовление СКПЭП в УЦ. В УЦ принимаются представленные Заявителем документы, вручаются готовые СКПЭП. Заявитель

может заранее предоставить в Удостоверяющий центр электронные копии документов, при условии подтверждения их соответствия оригиналам в УЦ.

5.2.1.3. Удостоверяющим центром в СКПЭП вносится информация на основании заявления. Если Владельцем сертификата является юридическое лицо, то наряду с наименованием такого юридического лица в СКПЭП может вноситься информация об Уполномоченном представителе. Удостоверяющий центр проверяет данные в Заявлении на изготовление СКПЭП на соответствие данным, содержащимся в иных представленных Заявителем документах, и устанавливает:

а. факт принадлежности документов предоставившему их лицу;

б. факт соответствия сведений, указанных в заявлении, представленным документам и, в необходимых случаях в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», информации, полученной из государственных реестров;

в. факт отсутствия явных признаков подделки документов.

5.2.1.4. В случае внесения в Сертификат персональных данных физического лица, Заявитель - физическое лицо или Уполномоченный представитель Заявителя предоставляет свое письменное согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия включен в заявление на выдачу Сертификата. Персональные данные, внесенные в Сертификат, становятся общедоступными в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Согласие должно быть подписано собственноручно лицом, данные о котором вносятся в Сертификат (субъектом персональных данных). Также согласие на обработку персональных данных может быть подписано представителем субъекта персональных данных, действующим на основании нотариальной доверенности, которая должна быть выдана от имени субъекта персональных данных, должна содержать полномочие на предоставление согласия на обработку персональных данных от имени субъекта персональных данных, а также должна соответствовать иным требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5.2.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов.

Форма заявления предоставляется клиенту в электронном виде. Актуальную форму заявления УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления Участников электронного взаимодействия.

Форма заявления на изготовление СКПЭП включает следующие сведения в зависимости от статуса заявителя.

Для владельца - юридического лица:

а. наименование организации;
б. ИНН, КПП, ОГРН;
в. юридический адрес с указанием области;
г. сведения об уполномоченном представителе:
- ФИО;
- паспортные данные - серия, номер паспорта, дата выдачи, код подразделения, дата и место рождения;
- СНИЛС;
- адрес электронной почты;
- должность;
- подразделение.

Для владельца - индивидуального предпринимателя:

а. наименование;
б. ИНН, ОГРНИП;
в. область, город/населенный пункт (согласно сведениям, об адресе места нахождения индивидуального предпринимателя);
г. сведения об уполномоченном представителе - владельце сертификата:
- ФИО;

- паспортные данные - серия, номер паспорта, дата выдачи, код подразделения, дата и место рождения;
- СНИЛС;
- адрес электронной почты.

Для владельца - физического лица:

а. ФИО;

б. паспортные данные - серия, номер паспорта, дата выдачи, код подразделения, дата и место рождения;

в. СНИЛС;

г. ИНН;

д. адрес электронной почты;

е. область, город/населенный пункт.

Использование факсимиле (клише подписи) на заявлении не допускается.

5.2.3. Порядок идентификации заявителя:

5.2.3.1. Идентификация гражданина Российской Федерации осуществляется при его личном присутствии по основному документу, удостоверяющему личность;.. Без его личного присутствия с использованием усиленной квалифицированной электронной подписи при наличии действующего сертификата; Путем предоставлении информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

5.2.3.2. Идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства.

5.2.3.3. Идентификация беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

5.2.3.4.

Документами, удостоверяющими личность гражданина РФ на территории РФ, являются:

а. паспорт гражданина РФ, удостоверяющий личность гражданина РФ на территории РФ, действует на территории РФ с 01 октября 1997 года;

б. паспорт моряка (с 2014 года - удостоверение личности моряка) является документом, удостоверяющим личность его владельца как за границей, так и в пределах РФ;

в. свидетельство о рождении является документом, удостоверяющим личность лиц (граждан РФ), не достигших 14-летнего возраста;

г. удостоверение личности военнослужащего РФ является документом, удостоверяющим личность и правовое положение военнослужащего РФ;

д. военный билет является документом, удостоверяющим личность солдат, матросов, сержантов и старшин, проходящих военную службу по призыву или контракту, а также курсантов военных образовательных учреждений профессионального образования на время их обучения;

е. временное удостоверение личности гражданина РФ по форме № 2-П - документ, удостоверяющий личность ограниченного срока действия (для утративших паспорт граждан, а также граждан, в отношении которых до выдачи паспорта проводится дополнительная проверка). Временное удостоверение выдается на срок, указанный в этом документе;

ж. служебное удостоверение работника прокуратуры;

з. документы, удостоверяющие личность иностранных граждан на территории РФ:

- паспорт иностранного гражданина (национальный паспорт или национальный заграничный паспорт) или иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина - для иностранных граждан, если они постоянно проживают на территории РФ;
- дипломатический паспорт иностранного гражданина является документом, удостоверяющим личность для иностранных граждан, временно пребывающих и проживающих на территории РФ;
- документ, выданный иностранным государством и признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность лица без гражданства;
- иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина или лица без гражданства;
- разрешение на временное проживание является документом, удостоверяющим личность иностранного гражданина или лица без гражданства (оформленное в виде документа установленной формы, выдаваемого в РФ лицу без гражданства, не имеющему документа, удостоверяющего личность). Данный документ подтверждает право иностранного гражданина или лица без гражданства временно проживать в Российской Федерации до получения вида на жительство;
- вид на жительство в РФ является документом, удостоверяющим личность лица без гражданства, подтверждающим его право на постоянное проживание в РФ;
- удостоверение беженца или свидетельство о рассмотрении ходатайства о признании беженцем на территории РФ является документом, удостоверяющим личность лица (иностранного гражданина или лица без гражданства), ходатайствующего о признании беженцем (статьи 4, 7 Федерального закона от 19.02.1993 № 4528-1 "О беженцах").

Все документы на иностранном языке должны быть апостилированы в консульстве (посольстве) РФ за границей (на территории того государства, где эти документы выданы), либо в консульстве (посольстве) иностранного государства (выдавшего документы, удостоверяющие личность) на территории РФ и иметь заверенный перевод на русский язык.

5.2.3.5. Требования к паспорту получателя:

а. паспорт гражданина РФ не должен быть просрочен;

б. документ не должен быть поврежден или испорчен;

5.2.4. Перечень документов, предоставляемых Заявителем в Удостоверяющий центр.

Заявитель, присоединяясь к настоящему Регламенту, предоставляет в Удостоверяющий центр следующие документы либо их надлежащим образом заверенные копии и (или) сведения из ник:

5.2.4.1. Для юридических лиц:

а. заявление на изготовление сертификата ключа проверки электронной подписи;

б. основной государственный регистрационный номер заявителя - юридического лица; (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);

в. номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);

г. основной документ, удостоверяющий личность заявителя;

е. страховой номер индивидуального лицевого счета заявителя- физического лица;

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

5.2.4.2. Для индивидуальных предпринимателей:

а. заявление на изготовление сертификата ключа проверки электронной подписи;

б. основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя (Заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);

в. основной документ, удостоверяющий личность заявителя;

д. страховой номер индивидуального лицевого счета заявителя - физического лица;

5.2.4.3. Для физических лиц:

а. заявление на изготовление сертификата ключа проверки электронной подписи;

б. основной документ, удостоверяющий личность заявителя;

в. страховой номер индивидуального лицевого счета заявителя - физического лица;

г. идентификационный номер налогоплательщика заявителя;

д. доверенность, подтверждающая право заявителя действовать от имени других лиц.

5.2.4.4. В случае, если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в Удостоверяющий центр документ соответствующей формы.

5.2.5. Порядок проверки достоверности документов и сведений, представленных заявителем

5.2.5.1. УЦ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем. Для заполнения квалифицированного сертификата Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов:

а. выписку из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;

б. выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;

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

5.2.5.3.В случае, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной Заявителем для включения в квалифицированный сертификат, и УЦ идентифицирован заявитель, УЦ осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата.

В противном случае, УЦ отказывает Заявителю в выдаче квалифицированного сертификата.

5.2.6. Порядок создания квалифицированного сертификата.

5.2.6.1. Регистрация Заявителя и изготовление первого сертификата.

Под регистрацией Заявителей понимается внесение регистрационной информации о Заявителях в Реестре УЦ.

Процедура регистрации Заявителя применяется в отношении физических лиц, обращающихся к услугам УЦ в части изготовления сертификатов ключей проверки ЭП Заявителей и/или формирования ключей ЭП и ключей проверки ЭП Заявителей с записью их на ключевой носитель.

5.2.6.2. Процедура создания ключей электронных подписей и выпуска СКПЭП:

1) Процедура создания в УЦ:

а. получение от Владельца заявления на изготовление СКПЭП;

б. проверка сведений, указанных в заявлении на изготовление СКПЭП и представленных документов;

в. в случае подтверждения достоверности сведений проводится проверка будущего ключевого носителя, допустимого эксплуатационной документацией к СКЗИ, на вирусы, при необходимости производится инициализация и создание ключа электронной подписи;

г. формирование запроса на СКПЭП;

д. выпуск СКПЭП;

е. размещение сертификата на носитель;

ж. внесение данных о выпущенных СКПЭП и ключевых носителях в журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

з. осуществление конвертования носителя с ключевой парой;

и. передача Владельцу носителя с ключевой парой под роспись в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

к. ознакомление Владельца со сведениями, содержащимися в сертификате.

2) Процедура создания клиентом самостоятельно:

а. получение от Владельца заявления на изготовление СКПЭП;

б. проверка сведений, указанных в заявлении на изготовление СКПЭП и представленных документов;

в. в случае подтверждения достоверности сведений Владельцу рекомендуется приступить к созданию ключа электронной подписи и запроса на сертификат на его персональном компьютере с использованием сертифицированных ФСБ России средств СКЗИ.

г. предоставление запроса на сертификат в УЦ для выпуска СКПЭП;

д. проверка сведений в запросе;

е. выпуск СКПЭП УЦ;

ж. ознакомление Владельца со сведениями, содержащимися в СКПЭП;

з. передача Владельцу;

и. размещение сертификата Владельцем на носитель.

5.2.7. Порядок выдачи квалифицированного сертификата.

5.2.7.1. Представитель УЦ выполняет процедуру идентификации лица, проходящего процедуру регистрации одним из способов, указанных в пункте 5.2.3.

5.2.7.2. Документы на электронных и бумажных носителях выдаются Заявителю с соблюдением требований по обеспечению конфиденциальности.

5.2.7.3. При получении квалифицированного сертификата Заявитель знакомится с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью заявителя. .

5.2.7.4. УЦ может выдать бланк сертификата на бумажном носителе по запросу владельца СКПЭП, подписанный Уполномоченным лицом УЦ.

5.2.7.5. УЦ одновременно с выдачей СКПЭП предоставляет руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств ЭП, содержащее информацию об условиях и о порядке использования электронных подписей и средств электронной подписи (СКЗИ), о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей.

5.2.7.6. При выдаче квалифицированного сертификата Заявитель получает:

а. ключ электронной подписи и СКПЭП;

б. бланк сертификата ключа проверки электронной подписи;

в. руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

5.2.8. Срок создания и выдачи квалифицированного сертификата с момента получения Удостоверяющим центром соответствующего заявления, а также условия для срочного создания и выдачи квалифицированного сертификата заявителю

Создание Сертификата производится в течение не более пяти рабочих дней с момента подачи заявления, при условии подтверждения всех фактов соответствия сведений в заявлении и соблюдения порядка оплаты за услуги.

5.3. Подтверждение действительности (подлинности) электронной подписи, использованной для подписания электронных документов.

5.3.1. Требования к заявлению на подтверждение действительности электронной подписи, в том числе перечень прилагаемых к такому заявлению документов

Подтверждение подлинности ЭП Удостоверяющего центра осуществляется на основании заявления Заявителя в свободной форме.

К заявлению прикладывается сертификат ключа проверки электронной подписи, подтверждение подлинности ЭП которого производится.

5.3.2. Срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе.

Срок проведения экспертизы составляет:

- 30 (тридцать) рабочих дней с момента поступления заявления в УЦ на безвозмездной основе;

- 2 рабочих дня, при условии поступления оплаты стоимости данной услуги на расчетный счет УЦ.

5.3.3. Порядок оказания услуги.

При проведении работ Удостоверяющим центром может быть запрошена дополнительная информация.

Процедура подтверждения действительности ЭП осуществляется с использованием специализированного программного обеспечения, входящего в состав сертифицированного средства УЦ, комиссией, состоящей из уполномоченных лиц УЦ. По согласованию сторон в комиссию могут входить представители заявителя или уполномоченные сотрудники правоохранительных органов. В ходе процедуры подтверждения действительности ЭП комиссией осуществляется проверка всех квалифицированных СКПЭП, на основании которых были сформированы электронные подписи на документах, определение даты формирования каждой электронной подписи в документах, проверку каждого квалифицированного СКПЭП в цепочке до квалифицированного СКПЭП Головного УЦ, проверку действительности всех квалифицированы СКПЭП на момент проверки и отсутствие их в CRL. Результатом работы комиссии является протокол проверки электронной подписи в электронном документе, в общем случае включающий в себя:

а. результат проверки квалифицированного СКПЭП или нескольких квалифицированных СКПЭП, необходимых для проверки ЭП;

б. проверка ЭП электронного документа с использованием одного или нескольких квалифицированных СКПЭП;

в. проверка действительности каждого квалифицированного СКПЭП в цепочке до квалифицированного СКПЭП ГоловногоУЦ.

5.4. Процедуры, осуществляемые при прекращении действия и аннулирования квалифицированного сертификата.

5.4.1. Основания прекращения действия квалифицированного сертификата:

1) истечении установленного срока его действия.

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

3) в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4) в иных случаях, установленных настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи

5.4.2. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

1) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

2) установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;

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

5.4.3. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) квалифицированного сертификата.

Заявление на прекращение действия сертификата может подаваться в Удостоверяющий центр в бумажной форме при личном прибытии Владельца в УЦ, либо почтовой или курьерской службой, а также в электронной форме, с подписью руководителя или лица, имеющего право действовать от имени организации по доверенности.

Срок внесения информации об аннулировании или прекращении действия сертификата в Реестр сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие СКПЭП прекращается с момента внесения записи об этом в реестр сертификатов.

5.5. Порядок ведения реестра квалифицированных сертификатов.

5.5.1. Формы ведения реестра квалифицированных сертификатов.

5.5.1.1. Реестр сертификатов ключей проверки ЭП ведётся в электронной форме.

Ведение реестра квалифицированных сертификатов включает в себя:

- внесение изменений в реестр квалифицированных сертификатов в случае изменения сведений;
- внесение в реестр квалифицированных сертификатов сведений о прекращении действия квалифицированных сертификатов.
- внесение в реестр квалифицированных сертификатов сведений о аннулировании квалифицированных сертификатов

5.5.1.2. Информация, внесенная в реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности аккредитованного удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

5.5.1.3. Хранение информации, содержащейся в реестре квалифицированных сертификатов, должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

5.5.1.4. Аккредитованный удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов.

5.5.1.5. Аккредитованный удостоверяющий центр обеспечивает защиту информации, содержащейся в реестре квалифицированных сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

5.5.1.6. Формирование и ведение реестра квалифицированных сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

5.5.1.7. Аккредитованный удостоверяющий центр обязан обеспечивать актуальность информации, содержащейся в реестре квалифицированных сертификатов.

5.5.2. Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре, формируется его резервная копия.

5.5.3. Сроки внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов.

Информация о прекращении действия квалифицированного сертификата вносится УЦ в реестр квалифицированных сертификатов в течение двенадцати часов с момента наступления обстоятельств, повлекших за собой прекращение действия квалифицированного сертификата или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр квалифицированных сертификатов.

5.6. Порядок технического обслуживания реестра квалифицированных сертификатов.

5.6.1. Максимальные сроки проведения технического обслуживания.

Плановое и внеплановое техническое обслуживание Реестра сертификатов осуществляется, как правило, во внерабочее время УЦ и не может превышать 12 (двенадцати) часов.

5.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания.

УЦ оповещает лиц, использующих Реестр сертификатов, о проведении планового или внепланового технического обслуживания Реестра сертификатов на официальном сайте УЦ.

6. Порядок исполнения обязанностей Удостоверяющего центра

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

Данная обязанность реализуется посредством предоставления владельцу, одновременно с самой подписью, руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, сущность которых сводится к определению обязанностей владельца сертификата, в том числе по обеспечению режима конфиденциальности информации.

6.2. Выдача по обращению заявителя средств электронной подписи.

6.2.1. Удостоверяющий центр по обращению заявителя выдает средства электронной подписи, отвечающие требованиям:

а. средства ЭП позволяют установить факт изменения подписанного электронного документа после момента его подписания;

б. средства ЭП обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки;

в. средства ЭП позволяют создать электронную подпись в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами электронной подписи.

6.2.2. При создании электронной подписи средства электронной подписи должны (не относится к средствам ЭП, используемым для автоматического создания ЭП):

а. показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;

б. создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

в. однозначно показывать, что электронная подпись создана.

6.2.3. При проверке электронной подписи средства электронной подписи должны (не относится к средствам ЭП, используемым для автоматической проверки ЭП):

а. показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного электронной подписью, включая визуализацию данной электронной подписи, содержащую информацию о том, что такой документ подписан электронной подписью, а также о номере, владельце и периоде действия сертификата ключа проверки электронной подписи;

б. показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

в. указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

6.2.4. Средства ЭП, предназначенные для создания электронных подписей в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

6.2.5. Средство электронной подписи должно противостоять угрозам, представляющим собой целенаправленные действия с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемой средством электронной подписи информации или с целью создания условий для этого.

Средство ЭП должно проводить аутентификацию субъектов доступа (лиц, процессов) к этому средству, при этом: при осуществлении доступа к средству электронной подписи аутентификация субъекта доступа должна проводиться до начала выполнения первого функционального модуля средства электронной подписи;

б. механизмы аутентификации должны блокировать доступ этих субъектов к функциям средства ЭП при отрицательном результате аутентификации.

6.2.6. Средство ЭП должно проводить аутентификацию лиц, осуществляющих локальный доступ к средству электронной подписи.

6.2.7. Средства электронной подписи аккредитованного Удостоверяющего центра и средства электронной подписи Заявителя/Владельца удовлетворяют требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ РФ от 27.12.2011 г. №796.

6.3. Обеспечение актуальности информации в реестре сертификатов и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий.

УЦ обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов, защиту информации от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий. Актуальность

обеспечивается путем своевременного внесения записи о выпуске и аннулировании СКПЭП в реестр квалифицированных сертификатов. Режим защиты является общим требованием в отношении всей сферы применения электронной подписи, он обеспечивается посредством применения специальных шифровальных средств, способствующих защите информации от несанкционированного проникновения.

6.4. Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением технического обслуживания реестра квалифицированных сертификатов.

УЦ обеспечивает доступность реестра КЭП круглосуточно, с использованием информационно-телекоммуникационных сетей к выданным УЦ квалифицированным сертификатам (uc.asu.ru), за исключением периодов планового или внепланового технического обслуживания реестра сертификатов.

6.5.Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.

6.5.1. Требования к обеспечению конфиденциальности.

Необходимо немедленно обратиться в удостоверяющий центр с заявлением на прекращение действия квалифицированного сертификата в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи. Запрещается:

а. оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, средства усиленной квалифицированной электронной подписи, после ввода ключевой информации;
б. вносить какие-либо изменения в программное обеспечение СКЗИ;
в. осуществлять несанкционированное копирование ключевых носителей;
г. разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным;
д. использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
е. записывать на ключевые носители постороннюю информацию;
ж. использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ;
з. ключи ЭП на ключевом носителе защищаются паролем (пин-кодом);
и. оставлять без присмотра ключи ЭП на ключевом носителе (на столе, подключенным к ПЭВМ и пр.)
к. допускать использование принадлежащих им ключей электронных подписей без их согласия;
л. применять ключ квалифицированной электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

6.5.2. Условия временного хранения ключей электронной подписи.

а. при хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Владелец несет персональную ответственность за хранение личных ключевых носителей;

б.запрещается оставлять без контроля вычислительные средства с установленным СКЗИ после ввода ключевой информации;

в. в случае централизованного хранения ключевых носителей в организации, эксплуатирующей СКЗИ, администратор безопасности (если он имеется) несет персональную ответственность за хранение личных ключевых носителей пользователей.

6.5.3. Сроки уничтожения ключей электронной подписи.

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), в том числе срок действия которых истек, уничтожаются путем переформатирования ключевых носителей

средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Срок уничтожения Владелец устанавливает самостоятельно.

6.6. Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации.

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

6.7. Осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации.

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

6.8. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие и аннулированных квалифицированных сертификатов.

Информация, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата предоставляется безвозмездно. Обращение подается при личном прибытии Владельца в УЦ в рабочее время УЦ, либо почтовой или курьерской службой.

Информация предоставляется в форме выписки из реестра квалифицированных сертификатов и направляется обратившемуся.

Выписка из Реестра позволяет определить действительность сертификатов ключей проверки ЭП Владельцев. Доступ к информации организован в соответствии с защитой персональных данных согласно требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и предоставляется при условии владения необходимыми данными из сертификата.

Для получения информации необходимо предоставить:

- серийный номер сертификата;

или

- ИНН Заявителя;
- СНИЛС Владельца;
- даты начала и окончания действия квалифицированного сертификата.

Также УЦ публикует перечень прекративших свое действие и аннулированных квалифицированных сертификатов, позволяющий определить действительность сертификатов ключей проверки ЭП Владельцев на официальном сайте uc.asu.ru.

Срок предоставления информации не превышает семи дней для направления информации почтовым отправлением и 24 часов для направления выписки посредством информационно- телекоммуникационных сетей.

7. Персональные данные

7.1. Обработка персональных данных Заявителей/Владельцев:

7.1.1. Цель обработки персональных данных в УЦ - исполнение требований Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»; изготовление и

хранение сертификатов ключей проверки ЭП, изготовление списков аннулированных сертификатов, ведение реестра выданных и аннулированных сертификатов, подтверждение неотрекаемости от подачи заявления и запроса на сертификат, от получения СКПЭП, установление личности заявителя - физического лица, обратившегося за получением сертификата ключа проверки электронной подписи (СКПЭП) и подтверждения правомочия обращаться за получением СКПЭП.

7.1.2. Обработка персональных данных в УЦ осуществляется на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

7.1.3. Персональные данные, обрабатываемые УЦ: фамилия, имя, отчество, реквизиты основного документа, удостоверяющего личность (серия, номер, код подразделения, дата выдачи), место работы, должность, служебный телефон, СНИЛС Заявителя/получателя СКПЭП, и иные сведения, необходимые для исполнения целей РегламентаУЦ.

7.1.4. Персональные данные, вносимые в СКПЭП относятся к категории общедоступных.

7.1.5. УЦ осуществляет действия по сбору, систематизации, накоплению, использованию, хранению, уточнению, обновлению, изменению, использованию, блокированию, уничтожению, передаче и распространению персональных данных Заявителя в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

7.1.6. УЦ не раскрывает третьим лицам и не распространяет персональные данные Заявителя без наличия письменного его согласия на раскрытие данной информации, за исключением случаев прямо установленных действующим законодательством Российской Федерации.

7.1.7. Согласие на обработку персональных данных Заявителя может быть отозвано по письменному заявлению в бумажном виде при личном прибытии Заявителя при удовлетворении которого, впоследствии Удостоверяющим центром аннулируются все выпущенные сертификаты данного Заявителя, при этом УЦ вправе не прекращать их обработку до окончания срока действия согласия.

7.1.8. Согласие вступает в силу с момента его подписания, действует до истечения срока хранения информации установленного п. 2 ст.15 Федерального закона от 04.06.2011 № 63-ФЗ «Об электронной подписи».

7.2 Архивное хранение информации и сведений Удостоверяющим центром.

На основании Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (ч.1 ст. 15) Аккредитованный удостоверяющий центр хранит следующую информацию:

1. реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;
2. сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;
3. сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

Хранение информации осуществляется в соответствии с ч.1 ст. 15, ч. 7 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

7.2.1. Документы УЦ, подлежащие архивному хранению, являются документами временного хранения, архив ведется в электронном и бумажном виде. Хранение документов в бумажном виде в УЦ осуществляется в течение всего периода их действия и 3 (три) года после их аннулирования или истечения срока их действия, в электронном виде - Сертификатов ключей проверки электронной подписи в течение всего срока деятельности УЦ, если иной срок не установлен нормативно-правовыми актами действующего законодательства Российской Федерации.

7.2.2. Архивному хранению подлежат следующие документы:

а. заявление на изготовление сертификата ключа подписи;

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

в. доверенность на получение ЭП;

г. доверенность на полномочного представителя;

д. СКПЭП (электронно);

е. сведения об ознакомлении с наддыми СКПЭП.

7.2.3. Хранение бумажного архива осуществляется в помещениях УЦ.

В одно дело группируются документы одного календарного года.

На титульном листе указывается период начала ведения дела и окончания.

Дело должно содержать около 250 листов, допускается чуть больше, чтобы комплект документов от одного клиента был полным.

После того, как в папке накоплено 250 листов, документы, составляющие дело, прошиваются в 2 прокола толстой нитью, заверяются подписью сотрудника ОКЗИ. На нить приклеивается лист бумаги 10*5 см, на котором ставится подпись сотрудника ОКЗИ с расшифровкой и печать, чтобы половина печати была размещена на приклеенном листе, а половина на основном.

На листе должно быть указано:

Прошито, пронумеровано, скреплено
печатью и
заверено подписью на____ (прописью) листах.
Ф.И.О./ _____ /
подпись

7.2.4. Уничтожение бумажного архива после истечения срока хранения документов.

Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией,
формируемой из числа сотрудников ОКЗИ УЦ и назначаемой приказом руководителя УЦ.

Комиссия составляет список архивных дел, по которым истек срок хранения. Список составляется по шаблону

<архив документов клиентов с ... по ...>.

Комиссия готовит Акт уничтожения документов.

Архивные дела, указанные в акте, уничтожаются полностью путем сжигания или разрезания (с помощью шредера) на мелкие части, склеивание которых невозможно для воссоздания документа.

Приложение №1
к Регламенту Удостоверяющего центра
ФГБОУ ВО «Алтайский государственный университет»

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Средства электронной подписи - шифровальные (криптографические) средства (СКЗИ), используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки, имеющие подтверждение соответствия требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» СКЗИ и средства ЭП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

2. Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

3. Для работы с СКЗИ и ключами ЭП привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Данные должностные лица, уполномоченные соответствующим приказом руководителя организации, несут персональную ответственность за:

а. сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;

б. сохранение в тайне содержания ключей ЭП и СКЗИ;

в. сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

4. В организации должны быть обеспечены условия хранения ключевых носителей ключей ЭП, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

5. Уполномоченные лица несут ответственность за то, чтобы на компьютере, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, - вирусы), которые могут нарушить функционирование программных СКЗИ. При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

6. Организация - обладатель конфиденциальной информации обязана вести журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с п. 26 Приказа ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». Неиспользованные или выведенные из действия ключевые документы подлежат уничтожению обладателем конфиденциальной информацией на месте, путем переформатирования ключевых носителей средствами ПО СКЗИ.

7. Не допускается:

а. разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

б. вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в другие ПЭВМ;

в. записывать на ключевом носителе постороннюю информацию;

г. вносить какие-либо изменения в СКЗИ и ключ ЭП;

д. использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей);

е. оставлять без контроля аппаратные средства, на которых эксплуатируются средства электронной подписи;

ж. оставлять без контроля носители ключевой информации;

з. сообщать PIN - код к ключевому носителю кому бы то ни было;

8. Действия в случае компрометации ключей:

а. под компрометацией ключей ЭП понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях, любые другие виды разглашения ключевой информации, в результате которых ключи ЭП могут стать доступными несанкционированным лицам и (или) процессам;

б. Владелец (уполномоченное лицо) самостоятельно должен определить факт компрометации ключа ЭП и оценить значение этого события для Владельца. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам владелец;

в. при компрометации ключа ЭП, владелец ключа должен немедленно поставить в известность представителей Удостоверяющего центра о факте компрометации. Заявление на прекращение действия

сертификата может подаваться в Удостоверяющий центр в бумажной форме при личном прибытии Заявителя в офис удостоверяющего центра, либо почтовой или курьерской доставкой, а также в электронной форме через личный кабинет, с подписью руководителя или лица, имеющего право действовать от имени организации по доверенности. Не позднее 1 часа после поступления заявления на прекращение действия сертификата ключа проверки, сертификат проверки ключа ЭП будет аннулирован. Последующая разблокировка прекратившего действие сертификата ключа проверки ЭП не возможна.

Для получения новых ключей уполномоченный представитель Заявителя, у которого были скомпрометированы ключи, должен обратиться в Удостоверяющий центр, имея при себе документы, необходимые для выпуска нового ключа ЭП. За выдачу новых ключей взимается оплата в соответствии с действующими тарифами на день оплаты.

9. PIN-код Владельца на носителе.

PIN-код для Рутокен, Рутокен ЭЦП 2.0 по умолчанию - 12345678.

PIN-код для eToken и JaCarta LT по умолчанию - 1234567890.

PIN-код для Jacarta PKI/ГОСТ и Jacarta-2 PKI/ГОСТ - 0987654321.

Владелец обязан изменить PIN-код при первом использовании ключевого носителя.

Надежный PIN-код должен состоять из смешанного набора цифровых и буквенных символов

10. Порядок установки и эксплуатации СКЗИ допускается в четком соответствии с документацией на используемое СКЗИ: https://www.cryptopro.ru/.