УТВЕРЖДАЮ

Генеральный директор
ОАО «ИнфоТеКС Интернет Траст»

А.Е. Прошин

"06" августа 2018 г.

РЕГЛАМЕНТ
предоставления Удостоверяющим центром ОАО «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки электронных подписей, не являющихся квалифицированными

2018 г.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Владелец сертификата ключа проверки электронной подписи (далее - владелец сертификата) - лицо, которому в установленном Законом порядке выдан сертификат ключа проверки электронной подписи.

Вручение сертификата ключа проверки электронной подписи - передача удостоверяющим центром или доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

Доверенное лицо Удостоверяющего центра – юридическое лицо или индивидуальный предприниматель, осуществляющее от имени Удостоверяющего центра функции по регистрации Пользователей Удостоверяющего центра и вручению сертификатов ключей проверки электронных подписей при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением сертификата.

Доверенный сервис электронной подписи - технологическое решение, реализованное в рамках информационной системы ОАО "ИнфоТеКС Интернет Траст", обеспечивающее централизованное безопасное хранение ключей и сертификатов ключей проверки ЭП Пользователей и удаленное выполнение операций по созданию усиленных неквалифицированных электронных подписей в интересах Пользователей.

Единая система идентификации и аутентификации (далее – ЕСИА) - федеральная государственная информационная система "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

Запрос на сертификат ключа проверки электронной подписи – электронное сообщение определенного формата и синтаксиса, содержащее необходимую информацию для создания сертификата.

Заявитель - лицо, обратившееся в Удостоверяющий центр за получением сертификата ключа проверки электронной подписи.

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

Ключ проверки электронной подписи (далее - ключ проверки ЭП) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка ЭП).

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (ключи электронной подписи).

Компрометация ключа электронной подписи - утрата доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам или подозрение, что ключи электронной подписи были временно доступны неуполномоченным лицам. К событиям, связанным с компрометацией ключа электронной подписи, относятся (включая, но не ограничиваясь):

- физическая утрата ключевого носителя;
- потеря ключевого носителя с его последующим обнаружением;
- передача ключа электронной подписи по открытым каналам связи;

– перехват ключа электронной подписи вредоносным программным обеспечением;
– несанкционированный доступ постороннего лица к устройству хранения ключа электронной подписи;
– случаи, когда невозможно достоверно установить, что произошло с ключевым носителем (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
– сознательная передача ключа электронной подписи постороннему лицу;
– увольнение сотрудников, имевших доступ к ключу электронной подписи;
– нарушение правил хранения ключевой информации.

Конфиденциальная информация - сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их владельца, а также информация, доступ к которой ограничен в соответствии с действующим законодательством РФ.

Несанкционированный доступ к информации - доступ к информации в нарушение должностных полномочий сотрудника или доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Плановая смена ключей электронной подписи - смена ключей электронной подписи, производимая в период действия ключей электронной подписи в соответствии с установленной в Удостоверяющем центре периодичностью, не вызванная компрометацией ключей электронной подписи.

Пользователь Удостоверяющего центра (далее - Пользователь) – лицо, пользующееся услугами Удостоверяющего центра и признающее настоящий Регламент.

Пункт обслуживания – место осуществления деятельности Удостоверяющего центра или Доверенного лица Удостоверяющего центра.

Регистрационные данные Пользователя - сведения, предоставляемые Заявителем в целях создания сертификата ключа проверки электронной подписи.

Реестр Пользователей – база данных Удостоверяющего центра, содержащая регистрационные данные Пользователей.

Реестр сертификатов – база данных Удостоверяющего центра, содержащая сведения о созданных Удостоверяющим центром сертификатах.

Сертификат ключа проверки электронной подписи (далее - сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи**.**

Список аннулированных сертификатов - отдельный раздел Реестра сертификатов, содержащий список уникальных номеров сертификатов ключей проверки ЭП, которые были аннулированы или действие которых на определенный момент времени было прекращено Удостоверяющим центром до истечения срока их действия, а также информацию о датах и об основаниях аннулирования или прекращения действия этих сертификатов.

Средства электронной подписи (далее - средства ЭП) - 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 (далее - средства УЦ) - программные и (или) аппаратные средства, используемые для реализации функций Удостоверяющего центра.

Удостоверяющий центр (далее - УЦ) - 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».

Электронный документ (далее - ЭД) - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронная подпись (далее - ЭП) - 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**.**

1. ВВЕДЕНИЕ

ОАО «ИнфоТеКС Интернет Траст» (далее - ОАО «ИИТ») выполняет функции Удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» и является ответчиком по всем юридическим вопросам деятельности Удостоверяющего центра.

1.1. Обзорная информация

Настоящий Регламент определяет механизмы предоставления услуг УЦ по созданию и выдаче сертификатов участникам информационного взаимодействия, соглашением между которыми установлены случаи признания электронных документов, подписанных усиленной неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, включая обязанности УЦ и пользователей УЦ (далее - стороны), процедуры взаимодействия сторон, форматы документов и данных, а также основные организационно-технические меры по обеспечению информационной безопасности при использовании ключевой информации и средств ЭП.

1.2. Идентификация Регламента

Наименование документа: «Регламент предоставления Удостоверяющим центром ОАО «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки электронных подписей, не являющихся квалифицированными».
Версия: 2.1.
Дата: 06.08.2018 г.

1.3. Публикация Регламента

Настоящий Регламент публикуется в электронном виде на сайте ОАО «ИИТ» по адресу **www.iitrust.ru**.

1.4. Заключение договора присоединения.

Настоящий Регламент со всеми приложениями к нему является договором присоединения в соответствии со ст. 428 Гражданского кодекса РФ.
Присоединение к настоящему Регламенту осуществляется путем подачи Заявителем заявления на создание неквалифицированного сертификата ключа проверки электронной подписи. С момента подачи заявления Заявитель считается присоединившимся к Регламенту и становится стороной Регламента. Факт присоединения Заявителя к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Заявления.

1.5. Область применения Регламента

1.5.1. Настоящий Регламент определяет порядок реализации функций УЦ ОАО «ИИТ» при создании и выдаче сертификатов участникам информационного взаимодействия, соглашением между которыми установлены случаи признания электронных документов, подписанных усиленной неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, а также для регулирования отношений, возникающих в процессе предоставления услуг УЦ.

1.6. Контактная информация Удостоверяющего центра ОАО «ИнфоТеКС Интернет Траст»

Юридический адрес: 127287, Москва, Старый Петровско-Разумовский проезд, дом. 1/23, стр.1.

Почтовый адрес: 127287, Москва, Старый Петровско-Разумовский проезд, дом. 1/23, стр.1.

Телефон: (495) 737-93-72, факс: (495) 737-93-73.

Телефон технической поддержки: (495) 737-33-69.

Телефон для справок, по России звонок бесплатный: 8-800-250-0-260 (кроме звонков из Москвы)

E-mail: supportiit@iitrust.ru

Web: www.iitrust.ru

1.7. Пользователи Удостоверяющего центра

1.7.1. Пользователями УЦ могут быть физические лица, в том числе зарегистрированные в качестве индивидуальных предпринимателей, и юридические лица, заключившие с УЦ договор об оказании услуг.

1.7.2. В случае, когда в качестве Пользователя выступает юридическое лицо, его интересы представляет физическое лицо, действующее на основании учредительных документов, либо доверенности.

1.8. Разрешение споров

1.8.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и сторона, присоединившаяся к Регламенту.

1.8.2. Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

1.8.3. Сторона, получившая от другой стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой стороне мотивированный отказ с указанием оснований отказа.

1.8.4. Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, и по которым не было достигнуто соглашение, разрешаются в судебном порядке в соответствии с законодательством РФ.

1.9. Прекращение деятельности Удостоверяющего центра

Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном законодательством РФ.

2. ОКАЗЫВАЕМЫЕ УСЛУГИ И РЕАЛИЗУЕМЫЕ ФУНКЦИИ

2.1. Услуги, оказываемые УЦ

2.1.1. Создание и выдача сертификатов лицам, обратившимся за их получением.

2.1.2. Предоставление средств ЭП, по обращению Пользователей.

2.1.3. Создание по обращениям Пользователей ключей ЭП, с гарантией обеспечения их конфиденциальности.

2.1.4. Аннулирование (отзыв) созданных УЦ сертификатов.

2.1.5. Предоставление информации из реестра сертификатов, созданных УЦ, в том числе информацию об аннулировании сертификата.

2.1.6. Осуществление по обращениям участников электронного взаимодействия проверку ЭП, созданных с использованием выданных УЦ сертификатов.

2.1.7. Осуществление по обращениям Пользователей подтверждения подлинности ЭП УЦ в выданных УЦ сертификатах.

2.1.8. Иные, связанные с использованием ЭП, услуги.

2.2. Функции, выполняемые УЦ

Функционирование УЦ обеспечивается выполнением следующих функций:

2.2.1. **Административные функции:**

2.2.1.1 Управление деятельностью УЦ.

2.2.1.2 Координация деятельности УЦ и Пунктов обслуживания.

2.2.1.3 Взаимодействие с Пользователями в части разрешения вопросов, связанных с применением предоставленных средств ЭП, ключей ЭП и сертификатов.

2.2.1.4 Взаимодействие с Пользователями в части разрешения вопросов подтверждения подлинности ЭП, созданных с использованием выданных УЦ сертификатов.

2.2.1.5 Взаимодействие с Пользователями в части разрешения вопросов, связанных с подтверждением ЭП УЦ в выданных УЦ сертификатах.

2.2.2. **Функции регистрации**

2.2.2.1 Установление личности заявителя - физического лица, обратившегося за получением сертификата.

2.2.2.2 Проверка правомочий лица, выступающего от имени заявителя - юридического лица, обращаться за получением сертификата.

2.2.2.3 Проверка достоверности регистрационных данных Пользователей на основании сведений, содержащейся в представленных Пользователем документах, а также полученных из государственных информационных ресурсов.

2.2.2.4 Ведение реестра выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей, в том числе включающего в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов, а также об основаниях прекращения действия или аннулирования сертификатов.

2.2.2.5 Иное взаимодействие с Пользователями в соответствии с настоящим Регламентом.

2.2.3. **Функции безопасности**

2.2.3.1 Выполнение комплекса организационно-технических мероприятий по защите ключей ЭП Удостоверяющего центра и Пользователей, а также информационных ресурсов УЦ, включающих, в частности, информацию, содержащуюся в реестре сертификатов, от несанкционированного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

2.2.3.2 Реализация средствами УЦ протокола аннулирования или прекращения действия сертификатов, формирования, обновления и публикации списков аннулированных сертификатов.

2.2.3.3 Установление сроков действия ключей ЭП и сертификатов.

2.2.3.4 Приостановление действия сертификатов при наличии у УЦ оснований полагать, что соответствующий ключ электронной подписи был скомпрометирован.

2.2.3.5 Прекращение действия сертификатов по заявлениям владельцев сертификатов.

2.2.3.6 Аннулирование сертификатов в связи с вступлением в силу решения суда, которым, в частности, установлено, что сертификат содержит недостоверную информацию.

2.2.3.7 Предоставление в любое время любому лицу доступа к актуальным спискам аннулированных сертификатов.

2.2.3.8 техническое обеспечение процедуры подтверждения подлинности ЭП, созданных с использованием выданных УЦ сертификатов;

2.2.3.9 техническое обеспечение процедуры подтверждения подлинности ЭП УЦ в выданных УЦ сертификатах.

3. ПРАВА

3.1. Права УЦ

УЦ имеет право:

3.1.1. Отказать Заявителям в регистрации и предоставлении услуг УЦ, с указанием причин отказа.

3.1.2. Отказать в создании сертификата зарегистрированным Пользователям, с указанием причин отказа.

3.1.3. С использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных Заявителем.

3.1.4. Прекратить действие сертификата без соответствующего заявления владельца сертификата в следующих случаях:

- если установлено, что сертификат содержит сведения, утратившие свою достоверность в связи с изменением регистрационных данных Пользователя;
- при наличии у Удостоверяющего центра существенных оснований полагать, что документы, представленные Заявителем в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность информации, включенной в данный сертификат;
- если установлено, что в результате технической ошибки сертификат содержит недостоверные или неполные сведения;
- в случае невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи и настоящим Регламентом.

3.1.5. Приостановить действие сертификата при наличии у УЦ оснований полагать, что соответствующий ключ электронной подписи был скомпрометирован, с уведомлением владельца сертификата и указанием обоснованных причин.

3.1.6. Осуществлять отправку сервисной информации в составе SMS-сообщений, направляемых на указанный Пользователем при регистрации абонентский номер мобильного телефона в целях получения Пользователем услуг Удостоверяющего центра.

3.2. Права Пользователей УЦ

Пользователи УЦ имеют право:

3.2.1. Обращаться в УЦ с целью получения ключа ЭП и сертификата.

3.2.2. Обращаться в УЦ с целью получения средств ЭП.

3.2.3. Использовать имеющиеся или предоставленные УЦ средства ЭП для формирования ключа ЭП и запроса на сертификат.

3.2.4. Получить копию сертификата на бумажном носителе, заверенную удостоверяющим центром.

3.2.5. Получить сертификат УЦ в форме электронного документа.

3.2.6. Обращаться в УЦ за подтверждением подлинности ЭП, созданных с использованием выданных УЦ сертификатов, в соответствии с порядком, определенным настоящим Регламентом.

3.2.7. Обращаться в УЦ за подтверждением подлинности ЭП УЦ в выданных УЦ сертификатах в соответствии с порядком, определенным настоящим Регламентом.

3.2.8. Обращаться в УЦ с заявлением на прекращение действия сертификата (в течение срока действия соответствующего ключа ЭП).

4. ОБЯЗАННОСТИ

4.1. Обязанности УЦ

4.1.1. По работе с ключами ЭП УЦ

4.1.1.1 УЦ обязан использовать ключ ЭП УЦ только для подписи создаваемых им сертификатов и списков аннулированных сертификатов.

4.1.1.2 УЦ обязан принимать меры по защите ключей ЭП УЦ в соответствии с положениями настоящего Регламента и нормативными правовыми актами РФ.

4.1.2. По регистрации пользователей

4.1.2.1 УЦ обеспечивает регистрацию Пользователей в реестре пользователей по заявлениям на услуги УЦ в соответствии с порядком, изложенном в настоящем Регламенте.

4.1.2.2 УЦ обязан не разглашать (не публиковать) регистрационные данные Пользователей, за исключением информации, включаемой в состав создаваемых сертификатов.

4.1.3. По созданию ключей ЭП Пользователей

4.1.3.1 УЦ создает ключи ЭП и ключи проверки ЭП на основании соответствующих обращений (заявлений) Пользователей с использованием средств ЭП, входящих в состав программно-технических средств УЦ, в том числе с использованием доверенного сервиса электронной подписи.

4.1.3.2 УЦ обязан обеспечить уникальность создаваемых ключей ЭП и ключей проверки ЭП в пространстве УЦ.

4.1.3.3 УЦ обязан информировать в письменной форме Пользователей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, а также о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

4.1.4. По созданию сертификатов

4.1.4.1 УЦ обеспечивает создание сертификатов по обращениям Пользователей, в соответствии с порядком и в форме, определенными настоящим Регламентом.

4.1.4.2 УЦ обязан обеспечить уникальность регистрационных (серийных) номеров создаваемых сертификатов.

4.1.5. По аннулированию или прекращению действия сертификатов

4.1.5.1 УЦ обязан аннулировать или прекратить действие сертификата в соответствии с порядком и на основаниях, указанным в разделах 6.3.4 и 6.3.5 настоящего Регламента.

4.1.5.2 УЦ обязан в течение 12 часов с момента возникновения обстоятельств, послуживших основанием для аннулирования или прекращения действия сертификата, внести сведения об аннулированном сертификате в список аннулированных сертификатов, с указанием даты, времени внесения сведений и причины аннулирования.

4.1.5.3 Датой и временем аннулирования сертификата признается дата и время внесения сведений об аннулированном сертификате в список аннулированных сертификатов.

4.1.5.4 УЦ обязан осуществлять публикацию списков аннулированных сертификатов в точках распространения, указанных в полях CRLDistributionPoints и AuthorityInfoAccess сертификата.

4.1.6. По ведению реестра сертификатов

4.1.6.1 УЦ обязан обеспечивать формирование и ведение реестра сертификатов в течение всего срока деятельности УЦ.

4.1.6.2 Реестр сертификатов ведется в электронном виде средствами УЦ и кроме информации, содержащейся в сертификатах, включает также информацию о датах прекращения действия или аннулирования сертификатов и об основаниях прекращения действия или аннулирования.

4.1.6.3 Сертификаты представляются в реестре сертификатов в форме электронных документов.

4.1.6.4 УЦ обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов.

4.2. **Обязанности Пользователя**

4.2.1. **Обязанности лиц, проходящих процедуру регистрации**

4.2.1.1 Лица, проходящие процедуру регистрации в УЦ, обязаны представить регистрационные данные в требуемом для создания сертификата объеме.

4.2.1.2 Лица, проходящие процедуру регистрации в УЦ, несут ответственность за достоверность предоставленных регистрационных данных.

4.2.2. **Обязанности Пользователя**

4.2.2.1 Принимать все возможные меры для предотвращения компрометации ключей ЭП, в том числе меры по обеспечению конфиденциальности аутентификационных данных, используемых для доступа к доверенному сервису электронной подписи.

4.2.2.2 Немедленно обращаться в УЦ с заявлением на прекращение действия сертификата в случае возникновения оснований предполагать компрометацию ключа ЭП или аутентификационных данных, используемых для доступа к доверенному сервису электронной подписи.

4.2.2.3 Извещать УЦ обо всех изменениях своих регистрационных данных в течение трех рабочих дней с момента регистрации изменений, а при изменении указанного при регистрации номера мобильного телефона - немедленно. При этом УЦ вправе затребовать у пользователя документы, подтверждающие изменение регистрационных данных.

4.2.2.4 Не применять ключ ЭП в случае его компрометации.

4.2.2.5 Не применять сертификат, содержащий информацию, не соответствующую регистрационным данным Пользователя.

4.2.2.6 Не использовать сертификат, заявление на аннулирование (отзыв) которого подано в УЦ.

4.2.3. **ОТВЕТСТВЕННОСТЬ**

4.2.4. **Ответственность УЦ**

4.2.4.1 УЦ несет ответственность за неисполнение либо ненадлежащее исполнение обязательств по настоящему Регламенту, за исключением случаев, предусмотренных п. 4.2.4.2 настоящего Регламента.

4.2.4.2 УЦ не несет ответственности за убытки, возникшие в связи с неисполнением или ненадлежащим исполнением УЦ обязательств по настоящему Регламенту в результате нарушения Пользователем настоящего Регламента, а также в случаях подделки, подлога либо иного искажения Пользователем или третьими лицами документов, удостоверяющих личность Заявителя - физического лица, подтверждающих правомочия лица, выступающего от имени Заявителя - юридического лица, или содержащих регистрационные данные Пользователя.

4.2.5. **Ответственность пользователя**

4.2.5.1 Пользователь несет ответственность за достаточность принимаемых им мер по обеспечению безопасности использования электронной подписи и средств ЭП, включая

защиту ключа ЭП и аутентификационных данных, используемых для доступа к доверенному сервису электронной подписи, от компрометации, потери, уничтожения, изменения или иного неавторизованного использования.

4.2.5.2 Пользователь несет ответственность за неизвещение УЦ об изменениях своих регистрационных данных.

4.2.5.3 Пользователь несет ответственность за использование скомпрометированного ключа ЭП и соответствующего сертификата ключа поверки ЭП в целях создания ЭП.

5. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

5.1. Виды конфиденциальной информации

5.1.1. Ключ ЭП владельца сертификата.

5.1.2. Аутентификационная информация, предоставляемая Пользователю в процессе прохождения процедуры регистрации и получения ключевых документов и/или средств ЭП.

5.1.3. Персональная и корпоративная информация пользователей, предоставленная в УЦ, не подлежащая распространению в составе сертификата.

5.2. Типы информации, не относящейся к конфиденциальной

5.2.1. Информация, не относящаяся к конфиденциальной информации, является открытой информацией.

5.2.2. Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации определяется решением УЦ.

5.2.3. Информация, включаемая в создаваемые УЦ сертификаты и списки аннулированных сертификатов, не считается конфиденциальной.

5.2.4. Также не считается конфиденциальной информация о настоящем Регламенте.

5.3. Предоставление конфиденциальной информации

УЦ не должен раскрывать информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам за исключением случаев:

- определенных в настоящем Регламенте;
- требующих раскрытия в соответствии с действующим законодательством РФ или при наличии судебного постановления.

6. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ

6.1. Регистрация Пользователей УЦ

6.1.1. Для регистрации в УЦ Заявитель подает в УЦ заявление на создание неквалифицированного сертификата ключа проверки ЭП, содержащее регистрационные данные Заявителя, включая информацию, подлежащую внесению в сертификат в соответствии с Федеральным законом "Об электронной подписи".

6.1.2. Заявление на создание неквалифицированного сертификата ключа проверки электронной подписи, подаваемое физическим лицом, должно содержать следующие сведения:

- фамилия, имя и отчество (если имеется);
- адрес регистрации по месту жительства;
- серия и номер паспорта гражданина РФ;
- дата выдачи паспорта гражданина РФ;

- наименование органа, выдавшего паспорт гражданина РФ;
- номер мобильного телефона;
- основной государственный регистрационный номер индивидуального предпринимателя, в случае если физическое лицо обращается за получением сертификата в качестве индивидуального предпринимателя.

6.1.3. Заявление на создание неквалифицированного сертификата ключа проверки, подаваемое юридическим лицом, должно содержать следующие сведения:

- наименование юридического лица;
- основной государственный регистрационный номер юридического лица;
- идентификационный номер налогоплательщика - юридического лица;
- сведения о документе, подтверждающем право лица, подписывающего заявление, действовать от имени юридического лица;
- фамилия, имя и отчество (если имеется) физического лица, указываемого в качестве владельца сертификата наряду с наименованием юридического лица;
- серия и номер паспорта гражданина РФ физического лица, указываемого в качестве владельца сертификата наряду с наименованием юридического лица;
- дата выдачи паспорта гражданина РФ физического лица, указываемого в качестве владельца сертификата наряду с наименованием юридического лица;
- наименование органа, выдавшего паспорт гражданина РФ физического лица, указываемого в качестве владельца сертификата наряду с наименованием юридического лица;
- номер мобильного телефона физического лица, указываемого в качестве владельца сертификата наряду с наименованием юридического лица.

6.1.4. Заявление на создание неквалифицированного сертификата ключа проверки электронной подписи может быть подано как в форме бумажного документа, так и в форме электронного документа.

6.1.5. Заявление на создание неквалифицированного сертификата ключа проверки электронной подписи в форме бумажного документа, подаваемое физическим лицом, должно быть подписано собственноручной подписью физического лица, а заявление, подаваемое юридическим лицом – собственноручной подписью лица, имеющего право действовать от имени юридического лица на основании учредительных документов юридического лица или доверенности.

6.1.6. Заявление на создание неквалифицированного сертификата ключа проверки электронной подписи в форме электронного документа подается через личный кабинет Пользователя в информационной системе Удостоверяющего центра. Идентификация и аутентификация субъектов доступа к личному кабинету осуществляется через ЕСИА, при этом заявитель должен иметь в ЕСИА подтвержденную учетную запись.

6.2. **Создание и выдача сертификата ключа проверки ЭП**

6.2.1. Создание сертификата осуществляется на основании регистрационных данных Пользователя.

6.2.2. Для получения сертификата Пользователь представляет документы, определенные требованиями информационных систем, для обеспечения информационного взаимодействия с участниками которых предназначен запрашиваемый сертификат.

6.2.3. Перед выдачей сертификата Удостоверяющий центр:

- устанавливает личность физического лица, в том числе выступающего от имени заявителя – юридического лица, обратившегося за получением сертификата, по основному документу, удостоверяющему личность, или через ЕСИА;
- осуществляет проверку правомочия лица, выступающего от имени заявителя - юридического лица, обращаться за получением сертификата;
- осуществляет проверку достоверности документов и сведений, представленных Пользователем в целях получения сертификата, используя при этом, в частности, документы, полученные из государственных информационных ресурсов:
  - выписка из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;
  - выписка из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;
  - выписка из Единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

6.2.4. В случае положительного результата действий, перечисленных в п. 6.2.3 настоящего Регламента, УЦ осуществляет:

- создание ключа электронной подписи и ключа проверки электронной подписи, в случае наличия соответствующего обращения со стороны Пользователя;
- создание и выдачу сертификата ключа проверки электронной подписи.

6.2.5. Одновременно с выдачей сертификата Пользователю выдаются средства электронной подписи, в случае наличия соответствующего обращения со стороны Пользователя.

6.2.6. В случае использования в информационной системе, для обеспечения информационного взаимодействия с участниками которой предназначен выдаваемый сертификат, доверенного сервиса электронной подписи, ключ ЭП и сертификат ключа проверки ЭП хранятся в информационной системе сервиса.

6.3. **Смена ключей ЭП Пользователя**

6.3.1. **Сроки действия ключей ЭП Пользователя**

Срок действия ключа ЭП, ключа проверки ЭП и, соответственно, сертификата ключа проверки ЭП Пользователя может составлять от 12 до 36 месяцев, в зависимости от требований информационной системы, для обеспечения информационного взаимодействия с участниками которой предназначен выдаваемый сертификат.

6.3.2. **Плановая смена ключей ЭП Пользователя**

6.3.2.1 Плановая смена ключей ЭП производится не ранее, чем за 40 (сорок), и не позднее, чем за 10 (десять) суток до окончания срока действия текущего сертификата (ключей ЭП и ключей проверки ЭП) Пользователя.

6.3.2.2 Создание новых ключа ЭП, ключа проверки ЭП и запроса на сертификат осуществляется Пользователем самостоятельно с использованием средств ЭП, установленных на его автоматизированном рабочем месте, или посредством доверенного сервиса электронной подписи.

6.3.2.3 Запрос на сертификат, сформированный с использованием средств ЭП, установленных на автоматизированном рабочем месте Пользователя, должен быть подписан электронной подписью Пользователя, основанной на действующем сертификате ключа проверки ЭП Пользователя, и передан в УЦ.

6.3.2.4 Создание сертификата для вновь сформированного ключа проверки ЭП Пользователя осуществляется УЦ не позднее 7 (семи) рабочих дней, следующих за рабочим днем, в течение которого УЦ был получен запрос на сертификат.

6.3.2.5 Если владельцем сертификата является юридическое лицо или индивидуальный предприниматель, то перед выдачей нового сертификата УЦ осуществляет проверку актуальности содержащейся в сертификате информации, используя документы, полученные из государственных информационных ресурсов:

- выписка из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;
- выписка из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;
- выписка из Единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

6.3.2.6 Если владельцем сертификата является юридическое лицо, то перед выдачей нового сертификата УЦ дополнительно осуществляет проверку правомочия лица, выступающего от имени юридического лица, обращаться за получением сертификата.

6.3.2.7 В случае если Пользователь не произвел плановую смену ключа ЭП в порядке и сроки, определенные в п.п. 6.3.2.1-6.3.2.3 настоящего Регламента, то создание нового ключа ЭП, ключа проверки ЭП и сертификата ключа проверки ЭП производится в порядке, определенном п. 6.2 настоящего Регламента.

6.3.3. **Внеплановая смена ключей ЭП Пользователя**

6.3.3.1 Внеплановая смена ключей ЭП производится:

- По инициативе Пользователя в период срока действия ключей ЭП, в следующих случаях:
  - при изменении регистрационных данных Пользователя в части их, содержащихся в сертификате;
  - при компрометации ключа ЭП Пользователя;
  - при компрометации аутентификационной информации Пользователя, предназначенной для получения доступа к доверенному сервису электронной подписи или для аутентификации в ЕСИА.
- При компрометации ключа ЭП УЦ.
- В иных случаях, вызванных обстоятельствами непреодолимой силы.

6.3.3.2 Создание и выдача сертификата ключа проверки ЭП при внеплановой смене ключа ЭП Пользователя производится в порядке, определенном в п. 6. 2 настоящего Регламента.

6.3.4. **Аннулирование сертификата**

6.3.4.1 Аннулирование сертификата осуществляется УЦ в следующих случаях:

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

6.3.4.2 До внесения в реестр сертификатов информации об аннулировании сертификата УЦ уведомляет владельца сертификата об аннулировании его сертификата путем направления уведомления в форме бумажного или электронного документа.

6.3.5. **Прекращение действия сертификата**

Удостоверяющий центр прекращает действие квалифицированного сертификата в следующих случаях:

- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме

электронного документа с ЭП владельца сертификата, поданного в УЦ по форме Приложения 2 к настоящему Регламенту;
- в случаях, указанных в пункте 3.1.4 настоящего Регламента.

6.3.6. **Приостановление действия сертификата**

6.3.6.1 Приостановление действия сертификатов осуществляется УЦ при наличии оснований полагать, что соответствующий ключ электронной подписи или аутентификационная информация Пользователя были скомпрометированы.

6.3.6.2 До внесения в реестр сертификатов информации о сертификате, действие которого было приостановлено, УЦ уведомляет владельца сертификата о приостановке действия его сертификата путем направления уведомления в форме бумажного или электронного документа.

6.4. Смена ключей ЭП УЦ

6.4.1. Сроки действия ключей ЭП УЦ

6.4.1.1 Срок действия ключа ЭП УЦ определяется в соответствии с требованиями эксплуатационной документации на средства ЭП УЦ и устанавливается равным 15 месяцам.

6.4.1.2 Срок действия ключа проверки ЭП и соответствующего сертификата УЦ устанавливается равным 72 месяцам.

6.4.1.3 Начало действия ключей ЭП УЦ исчисляется с даты и времени начала действия соответствующего сертификата.

6.4.2. Плановая смена ключей ЭП УЦ

6.4.2.1 Плановая смена ключей ЭП УЦ и соответствующего сертификата УЦ выполняется не позднее определенного в п. 6.4.1 срока действия текущего ключа ЭП УЦ.

6.4.2.2 Процедура плановой смены ключей ЭП УЦ выполняется в порядке, определенном эксплуатационной документацией на средства УЦ.

6.4.3. Внеплановая смена ключей ЭП УЦ

6.4.3.1 Внеплановая смена ключей ЭП УЦ производится в случае компрометации или угрозы компрометации ключа ЭП УЦ.

6.4.3.2 Внеплановая смена ключей ЭП УЦ выполняется в порядке, определенном эксплуатационной документацией на средства УЦ.

6.4.3.3 При выполнении внеплановой смены ключей ЭП УЦ сертификат ключа проверки ЭП, соответствующий скомпрометированному ключу ЭП УЦ должен быть аннулирован и внесен в список аннулированных сертификатов. Также должны быть проведены работы по внеплановой смене ключей ЭП пользователей, сертификаты которых подписаны ЭП, созданными с использованием скомпрометированного ключа ЭП УЦ.

6.5. Подтверждение подлинности ЭП Пользователя в ЭД

6.5.1. Подтверждение подлинности ЭП в ЭД осуществляется УЦ по обращению Пользователей УЦ на основании заявления в простой письменной форме на подтверждение подлинности ЭП в ЭД.

6.5.2. Заявление на подтверждение подлинности ЭП в ЭД подается Пользователем в УЦ или Пункт обслуживания лично.

6.5.3. Заявление на подтверждение подлинности ЭП в ЭД должно содержать информацию о дате и времени создания ЭП в ЭД.

6.5.4. В случае использования для создания ЭП средства ЭП, не входящего в состав доверенного сервиса электронной подписи, бремя доказывания достоверности даты и времени создания ЭП в ЭД возлагается на заявителя.

6.5.5. Обязательным приложением к заявлению на подтверждение ЭП в ЭД является внешний носитель информации, содержащий ЭД с ЭП в формате PKCS#7.

6.5.6. Срок проведения работ по подтверждению подлинности ЭП в ЭД составляет 10 (десять) рабочих дней с момента поступления заявления в УЦ.

6.5.7. В ходе проведения работ по подтверждению подлинности ЭП в ЭД Удостоверяющим центром может быть запрошена дополнительная информация.

6.5.8. Результатом проведения работ по подтверждению подлинности ЭП в ЭД является ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника и печатью УЦ.

Ответ должен содержать:

- результат проверки средством ЭП, имеющем подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом "Об электронной подписи", принадлежности ЭП в ЭД владельцу сертификата и отсутствия искажений в подписанном данной ЭП ЭД;
- детальный отчет по выполненной проверке (экспертизе).

6.5.9. Детальный отчет по выполненной проверке должен включать следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или экспертной комиссии (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- вопросы, поставленные перед экспертом или экспертной комиссией;
- объекты исследований и материалы по заявлению, представленные для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения.

6.5.10. Материалы и документы, иллюстрирующие заключение эксперта или экспертной комиссии, прилагаются к детальному отчету и являются его составной частью.

6.5.11. Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами экспертной комиссии.

6.6. **Порядок предоставления доступа к реестру сертификатов Удостоверяющего центра**

6.6.1. Информация, содержащаяся в реестре сертификатов Удостоверяющего центра, предоставляется любому лицу по его запросу, направляемому в Удостоверяющий центр по электронной почте либо через сайт Удостоверяющего центра.

6.6.2. Запрос должен содержать реквизиты сертификата, информация о котором запрашивается, в объеме, необходимом и достаточном для осуществления поиска в реестре сертификатов, включая, но не ограничиваясь:

- полное наименование и идентификационный номер налогоплательщика – для юридического лица;
- фамилия, имя, отчество – для физического лица.

6.6.3. В случае если в реестре сертификатов содержится информация о сертификатах, владельцами которых являются физические лица с полностью совпадающими фамилией, именем и отчеством, Удостоверяющий центр вправе запросить дополнительную информацию, позволяющую однозначно определить сертификат, информация о котором запрашивается.

6.6.4. Удостоверяющий центр предоставляет информацию, содержащуюся в реестре сертификатов, в течении 8 (восьми) рабочих часов с момента получения соответствующего запроса.

7. СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

УЦ формирует списки аннулированных сертификатов в соответствии с рекомендациями IETF RFC 5280 (2008) "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

8. РАЗРЕШЕНИЕ СПОРОВ

8.1. Сторонами в споре, в случае его возникновения, считаются УЦ и сторона, присоединившаяся к Регламенту.

8.2. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, стороны должны руководствоваться законодательством РФ.

8.3. Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

8.4. Сторона, получившая от другой стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой стороне мотивированный отказ с указанием оснований отказа.

8.5. Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, в том числе касающиеся его заключения, действия, исполнения, изменения, прекращения или действительности, и по которым не было достигнуто соглашение, разрешаются в судебном порядке в соответствии с законодательством РФ.

9. ОСНОВЫ ДЕЯТЕЛЬНОСТИ И МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УЦ

9.1. УЦ имеет разрешение (лицензии) на осуществление всех видов деятельности, связанных с предоставлением услуг УЦ (см. раздел 2.1 настоящего Регламента).

9.2. Документы, регламентирующие обеспечение мер по защите информации УЦ введены в действие соответствующими приказами.

9.3. Для обеспечения своей деятельности по созданию и выдаче сертификатов ключей проверки электронных подписей, не являющихся квалифицированными, УЦ использует средства УЦ, включая средства ЭП, входящие в состав доверенного сервиса электронной подписи.

10. ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

10.1. Оригинал настоящего Регламента формируется форме бумажного документа и заверяется собственноручной подписью руководителя УЦ и печатью УЦ.

10.2. Внесение изменений (дополнений) в Регламент производится Удостоверяющим центром в одностороннем порядке.

10.3. Все изменения (дополнения), вносимые в Регламент, вступают в силу с момента публикации актуальной версии Регламента в электронном виде в репозитории ОАО «ИИТ» по адресу www.iitrust.ru.

11. ПРИЛОЖЕНИЯ

Приложение 1. Информация об условиях и порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

Приложение 2. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи.

Приложение 1
к Регламенту предоставления Удостоверяющим центром
ОАО «ИнфоТеКС Интернет Траст» услуг по созданию и
выдаче сертификатов ключей проверки электронных
подписей, не являющихся квалифицированными

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

1. Риски, связанные с использованием электронной подписи.

К основным рискам, связанным с использованием электронной подписи, относятся:

1.1. Несанкционированное подписание электронного документа электронной подписью, которое может быть произведено в результате:

- компрометации ключа электронной подписи;
- подмены подписываемого документа в результате работы на компьютере вредоносного программного обеспечения.

1.2. Негативные последствия, вызванные невозможностью подписания электронного документа электронной подписью, обусловленной следующими событиями:

- уничтожение (удаление с ключевого носителя) ключа и/или сертификата ключа проверки электронной подписи;
- неисправность ключевого носителя, на котором хранятся ключ и/или сертификата ключа проверки электронной подписи;
- блокировка ключевого носителя или блокировка доступа к функциям доверенного сервиса электронной подписи, вызванная неоднократным вводом некорректного кода доступа (пароля или ПИН-кода);
- физическая утрата ключевого носителя.

1.3. Риск фальсификации электронной подписи.

Данный риск является скорее гипотетическим, но при использовании несертифицированного средства ЭП или использовании средства ЭП, полученного нелегально, в том числе и не определенным для данного средства способом, может породить следующие реальные риски:

- Риски отказа автора от своей электронной подписи под электронным документом или признания электронной подписи под электронным документом недействительной, которые могут быть аргументированы возможностью подделки электронной подписи при использовании несертифицированных или полученных нелегальным путем средств ЭП (т.е. не обладающих гарантированной криптографической стойкостью).
- Риск отказа автора от содержания подписанного электронной подписью электронного документа, которое может быть аргументировано возможностью модификации подписываемого документа при использовании несертифицированных или полученных нелегальным путем средств ЭП (т.е. обладающего недекларированными возможностями).

В целях снижения рисков, связанных с использованием электронной подписи, необходимо выполнение комплекс организационно-технических и административных мер по обеспечению безопасности использования электронной подписи и средств электронной подписи.

2. Порядок получения сертифицированных средств ЭП*.

Возможны два легальных способа получения средств ЭП:

2.1. Путем загрузки дистрибутива средства ЭП из точки распространения на Интернет-ресурсе производителя. Такой способ получения средства электронной подписи является легитимным

только в отношении тех средств ЭП, распространение которых через сеть Интернет согласовано с Федеральной службой безопасности РФ. В настоящее время легитимно распространяемым через сеть Интернет средством ЭП является ViPNet CSP.

2.2. На инсталлирующих средства ЭП носителях информации. Распространение инсталлирующих средств ЭП носителей осуществляется организациями, имеющими лицензию Федеральной службы безопасности РФ на выполнение соответствующего вида работ и оказания услуг в отношении шифровальных (криптографических) средств.

3. Организация работ по обеспечению безопасности использования электронной подписи и средств электронной подписи.

3.1. Безопасность использования электронной подписи и средств ЭП должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

3.2. Правом доступа к рабочим местам с установленными средствами ЭП должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Каждый пользователь, применяющий средства ЭП, должен быть ознакомлен с настоящей Информацией и документацией на средства ЭП.

4. Требования по размещению технических средств с установленными средствами ЭП.

При размещении технических средств с установленными на них средствами ЭП:

4.1. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средствами ЭП, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.

4.2. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключи электронной подписи.

5. Требования по установке средств ЭП, а также общесистемного и специального программного обеспечения*.

5.1. Установку общесистемного и специального программного обеспечения (далее – ПО), а также средств ЭП, должны осуществлять лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и средство ЭП.

5.2. При установке средств ЭП следует:

- На технических средствах, предназначенных для работы со средствами ЭП, использовать только лицензионное программное обеспечение фирм - изготовителей.
- На компьютере не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода средств ЭП и приложений, использующих средства ЭП, а также для просмотра кода и областей памяти, используемой средствами ЭП, в процессе обработки средствами ЭП информации и/или при загруженной ключевой информации.
- Предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлены средства ЭП (например, путем опечатывания системного блока и разъемов компьютера).

---

* При использовании доверенного сервиса электронной подписи необходимость получения и установки средств ЭП на клиентском рабочем месте отсутствует.

- Программное обеспечение, устанавливаемое на компьютер с установленным средством ЭП, не должно содержать возможностей, позволяющих:
  - модифицировать содержимое произвольных областей памяти;
  - модифицировать собственный код и код других программ;
  - модифицировать память, выделенную для других программ;
  - передавать управление в область собственных данных и данных других программ;
  - несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
  - модифицировать настройки операционной системы (далее – ОС);
  - использовать недокументированные фирмой-разработчиком функции ОС.

6. Требования по защите от несанкционированного доступа при эксплуатации средств ЭП.

При организации работ по защите информации от несанкционированного доступа (далее – НСД) необходимо учитывать следующие требования:

6.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS (basic input/output system) и т.д.), использовать пароли, сформированные в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 года.

6.2. Запрещается:

- оставлять без контроля компьютер, на котором эксплуатируются средства ЭП, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение средств ЭП;
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств ЭП;
- записывать на ключевые носители постороннюю информацию.

6.3. Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

6.4. Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.

6.5. При подключении компьютера с установленными средствами ЭП к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

6.6. При использовании средств ЭП на компьютерах, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют средства ЭП, и к компонентам средств ЭП со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

6.7. Необходимо организовать и использовать комплекс мероприятий антивирусной защиты.

6.8. Необходимо исключить одновременную работу средств ЭП различных производителей.

6.9. К работе со средствами ЭП допускаются лица, изучившие настоящее Руководство и пользовательскую документацию на средства ЭП.

7. Действия при компрометации ключей электронной подписи.

7.1. Пользователь самостоятельно должен определить факт компрометации ключа электронной подписи, оценить значение этого события и выполнить мероприятия по розыску и локализации последствий компрометации ключа электронной подписи.

7.2. При компрометации ключа электронной подписи пользователь должен немедленно сообщить в Удостоверяющий центр о факте компрометации. Информация о компрометации должна передаваться в Удостоверяющий центр способом, определенным Регламентом Удостоверяющего центра. По получении информации о компрометации ключа электронной подписи Удостоверяющий центр осуществляет аннулирование сертификата ключа проверки электронной подписи, в результате чего создание действительной электронной подписи с использованием скомпрометированного ключа электронной подписи становится невозможным.

Приложение 2
к Регламенту предоставления Удостоверяющим центром ОАО «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки электронных подписей, не являющихся квалифицированными

Удостоверяющий Центр
ОАО «ИнфоТеКС Интернет Траст»

Заявление
на прекращение действия сертификата ключа проверки электронной подписи

Прошу прекратить действие выданного УЦ ОАО «ИнфоТеКС Интернет Траст» сертификата ключа проверки электронной подписи со следующими реквизитами:

Серийный номер сертификата: _____

ФИО владельца сертификата (полностью): _____

Наименование организации (для юридических лиц):

_____

ИНН: (для юридических лиц): _____

в связи с _____
(причина прекращения действия сертификата)

_____

_____

_____

От Пользователя:

_____ /_____/
подпись фамилия, инициалы

"____" _____ 20__г.

М.П.