УТВЕРЖДЕНО

Приказом №УЦ-1/13

от 2 сентября 2013 г.

РЕГЛАМЕНТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

общества с ограниченной ответственностью

«Сайфер Линк»

Редакция 1.0

Оглавление

1. ВВЕДЕНИЕ

Настоящий регламент описывает порядок предоставления услуг удостоверяющего центра и правила их использования участниками электронного взаимодействия.

Настоящий регламент является соглашением, налагающим обязательства на все вовлеченные стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг удостоверяющего центра.

Настоящий регламент подготовлен в соответствии с рекомендациями RFC 3647. Certificate Policy and Certification Practices Framework.

1.1. Обзор

Регламент определяет правила, механизмы и условия предоставления и использования услуг удостоверяющего центра, включая права, обязанности и ответственность владельцев и пользователей сертификатов ключей проверки электронной подписи (далее, если контекст явно не подразумевает иного толкования – сертификатов), протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, включая, но не ограничиваясь, такие операции, как выпуск, использование, обновление и отзыв сертификатов.

1.2. Наименование и идентификация документа

Наименование документа: Регламент удостоверяющего центра общества с ограниченной ответственностью «Сайфер Линк».

Объектный идентификатор: не присвоен.

Версия документа: 1.0

Дата вступления в действие: 02.09.2013

Актуальная редакция настоящего документа доступна по ссылке: http://cilink.ru/docs

1.3. Участники электронного взаимодействия

1.3.1. Удостоверяющий центр

Удостоверяющий центр – лицо, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, в соответствии с Федеральным законом Российской Федерации от 06 апреля 2011 года №63-ФЗ «Об электронной подписи».

1.3.2. Центр регистрации

Центр регистрации – лицо, уполномоченное удостоверяющим центром проводить процедуру регистрации лиц, подавших заявления на выдачу сертификата, инициировать и рассматривать заявления на выдачу, обновление и отзыв сертификатов от имени удостоверяющего центра.

1.3.3. Владелец сертификата

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном законом порядке выдан сертификат ключа проверки электронной подписи (п. 4 ст. 2 №63-ФЗ).

1.3.4. Прочие участники электронного взаимодействия

Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане (п. 11 ст. 2 №63-ФЗ).

1.4. Использование сертификатов

1.4.1. Допустимое использование сертификата

Сертификаты могут использоваться в соответствии с указанными в них сведениями для электронной подписи электронных документов.

1.4.2. Недопустимое использование сертификата

Сертификаты не могут быть использованы в системах, критичных к отказоустойчивости, таких, как объекты авиации, ядерной энергетики, и т.п.

1.5. Управление документом

1.5.1. Организация, ответственная за содержание документа

Общество с ограниченной ответственностью «Сайфер Линк»
191167, Санкт-Петербург, Шпалерная ул. 51 лит. "А".

1.5.2. Контактная информация

Телефон: +7 (812) 676 8670
Сайт: http://cilink.ru

1.5.3. Лица, утверждающие изменения

Изменения регламента утверждаются уполномоченным лицом удостоверяющего центра.

1.5.4. Процедура утверждения изменений

Изменения в регламент вносятся сотрудниками удостоверяющего центра или уполномоченным федеральным органом и утверждаются уполномоченным лицом удостоверяющего центра.

Официальным уведомлением участников электронного взаимодействия об утверждении изменений регламента является его публикация на интернет-сайте удостоверяющего центра по адресу: http://cilink.ru/docs.

Все изменения, вносимые в регламент, вступают в силу и становятся обязательными к исполнению всеми потребителями услуг удостоверяющего центра немедленно после их публикации.

1.6. Определения и сокращения

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

1.6.2. 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.

1.6.3. Квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган).

1.6.4. Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

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

1.6.6. Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 6 апреля 2011 года №63-ФЗ «Об электронной подписи».

1.6.7. Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

1.6.8. Средства удостоверяющего центра – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

1.6.9. Корпоративная информационная система – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

1.6.10. Информационная система общего пользования – информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

1.6.11. COC – список отозванных (аннулированных) сертификатов.

1.6.12. OCSP – online certificate status protocol, протокол онлайновой проверки статуса сертификата.

1.6.13. TSP – time stamping protocol, протокол штампов времени.

2. ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ

2.1. Реестр выданных сертификатов

Удостоверяющий центр ведет реестр выданных сертификатов, обеспечивает его актуальность и возможность свободного доступа к нему участников электронного взаимодействия в соответствии с законодательством.

2.2. Публикация реестра выданных сертификатов

Удостоверяющий центр публикует реестр выданных сертификатов и осуществляет по обращениям участников электронного взаимодействия подтверждение подлинности электронной подписи в электронном виде.

Подтверждение подлинности электронной подписи производится путем предоставления сведений о статусе выданных сертификатов и сертификатов уполномоченных лиц удостоверяющего центра участникам электронного взаимодействия. Каждый сертификат, выданный удостоверяющим центром, содержит ссылку на раздел интернет-сайта, в котором опубликованы сертификаты уполномоченных лиц удостоверяющего центра и списки отозванных сертификатов. Указанные сведения позволяют при использовании средств электронной подписи, реализующих функцию проверки электронной подписи, получать подтверждение подлинности электронной подписи в электронном документе.

Сертификаты уполномоченных лиц удостоверяющего центра размещаются на интернет-сайте удостоверяющего центра в соответствующем разделе, а также на портале уполномоченного федерального органа http://reestr-pki.ru.

2.3. Время и частота публикаций реестра

Выданные сертификаты вносятся в реестр и публикуются не позднее даты начала их действия.

Сведения о статусе сертификатов публикуются в соответствии с настоящим регламентом.

2.4. Доступ к реестрам

Сведения, публикуемые на интернет-сайте удостоверяющего центра, предоставляются участникам электронного взаимодействия в режиме свободного доступа с правами «только для чтения».

Удостоверяющий центр осуществляет защиту от несанкционированного доступа к реестру.

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1. Имена (наименования)

3.1.1. Типы имен

Удостоверяющий центр выдает сертификаты, соответствующие стандарту ITU-T X.509v3. Выданные сертификаты содержат в полях «Субъект» и «Издатель» сведения, представленные в соответствии с рекомендациями ITU-T X.501 (Distinguished Names).

Наименования, которые удостоверяющий центр вносит в сертификаты, указываются в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», приказом ФСБ от 27 декабря 2011 г. N 795 "ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ФОРМЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ", а так же с рекомендациями Министерства связи и массовых коммуникаций, размещенными по адресу http://reestr-pki.ru/DOCS/Recomend_v1_9.zip.

3.1.2. Необходимость в значимых именах (наименованиях)

Указанные в сертификате сведения однозначно ассоциированы с владельцем сертификата. В частности, в тех случаях, когда в поле Common Name в качестве псевдонима указан номер договора владельца сертификата с удостоверяющим центром, владельцем сертификата является лицо, подписавшее договор, которое идентифицируется реквизитами

основного документа, удостоверяющего личность, копия которого была предоставлена владельцем сертификата одновременно с подписанием договора.

3.1.3. Использование псевдонимов

В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат.

В случаях, когда сертификат явно не содержит фамилии, имени и отчества владельца в соответствующем поле, считается, что в этом сертификате ключа подписи указан псевдоним.

3.1.4. Правила интерпретации различных форм имен (наименований)

Нет условий.

3.1.5. Уникальность имен (наименований)

В случаях полного совпадения сведений, содержащихся в нескольких сертификатах, принадлежащих разным владельцам, в них вносятся дополнительный атрибут (серийный номер), позволяющий однозначно идентифицировать их владельцев.

3.1.6. Использование торговых марок

Нет условий.

3.2. Процедура первичной регистрации

3.2.1. Способ доказательства факта обладания правом доступа к ключам электронной подписи

Способом доказательства факта обладания правом доступа к ключам электронной подписи является использование для этих целей специального устройства со встроенным модулем идентификации (например смарт-карты с модулем идентификации) или специальных реквизитов (кодов), а так же паролей, требования к наличию и сложности которых устанавливаются владельцами информационных систем, в которых коды и пароли используются.

3.2.2. Процедура аутентификации физического лица (представителя юридического лица)

При подаче заявления, заявитель – физическое лицо предоставляет основной документ, удостоверяющий личность, а так же свидетельство СНИЛС. Удостоверяющий центр имеет право выполнять копирование предъявленного документа для последующей передачи в архивное делопроизводство.

Удостоверяющий центр имеет право проверки данных основного документа, удостоверяющего личность и СНИЛС с использованием установленных законом средств СМЭВ.

Проверке могут подвергаться все сведения, указанные в заявлении. Удостоверяющий центр вправе отказать заявителю в выдаче сертификата, а так же аннулировать выданный сертификат в случае обнаружения ложных / не соответствующих действительности сведений

3.2.3. Сведения, указанные в заявлении, не подвергающиеся проверке

Удостоверяющий центр оставляет за собой право осуществлять проверку всех сведений, указанных в заявлении на выдачу сертификата.

3.2.4. Дополнительные условия аутентификации

Удостоверяющий центр вправе требовать от заявителя представления дополнительных документов, подтверждающих сведения, указанные в заявлении.

В случае подачи заявления законным представителем заявителя, законный представитель должен представить доверенность на осуществление действий от имени заявителя.

3.2.5. Подтверждение полномочий владельца сертификата

Нет условий.

3.2.6. Взаимодействие с владельцами сертификатов, выданными другими удостоверяющими центрами

Устанавливается законодательством РФ в области электронной подписи.

3.3. Идентификация и аутентификация заявителя при смене ключей

3.3.1. Идентификация и аутентификация в случае плановой (очередной) смены ключей

В случаях, когда у удостоверяющего центра имеются сведения о смене владельца и / или компрометации ключей электронной подписи и / или кодов (паролей) доступа к средствам электронной подписи владельца сертификата, процедура аутентификации в случае плановой смены ключей может проводиться в порядке, описанном в п.3.2.

3.3.2. Идентификация и аутентификация в случае смены ключей после отзыва (аннулирования)

Процедура проводится в порядке, описанном в п. 3.2.

3.3.3. Идентификация и аутентификация заявителя при подаче заявления на отзыв (аннулирование) сертификата

До фактического выполнения процедуры отзыва сертификата ключа подписи, удостоверяющий центр проверяет тот факт, что заявление на отзыв сертификата исходит от лица, уполномоченного подавать заявления в соответствии с п.4.9.2.

4. ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА

4.1. Заявление на выдачу сертификата

4.1.1. Лица, имеющие право подавать заявления на выпуск сертификатов

Заявление на выдачу сертификата имеют право подавать физические и юридические лица и их законные представители.

4.1.2. Процедура и обязательства по регистрации

Под регистрацией понимается внесение регистрационной информации о владельце сертификата в реестр удостоверяющего центра.

Процедура регистрации владельца сертификата выполняется в отношении физических и юридических лиц, обращающихся к услугам удостоверяющего центра в части изготовления сертификатов и/или изготовления ключей электронной подписи и ключей проверки электронной подписи.

Лицо, желающее пройти процедуру регистрации должно подтвердить свое полное и безоговорочное присоединение к настоящему регламенту, а также заполнить и передать в удостоверяющий центр или центр регистрации заявление на выдачу сертификата, предоставив документальное подтверждение сведений, указанных в заявлении.

Владелец сертификата письменно выражает согласие с обработкой своих персональных данных удостоверяющим центром и признает, что персональные данные, вносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным в соответствии с законодательством.

Заявления, поданные от физического лица, должны обязательно содержать следующие сведения:
- фамилию, имя и отчество;
- серия паспорта и номер паспорта, кем и когда выдан;
- адрес электронной почты;
- контактные телефоны;
- номер свидетельства СНИЛС.

Удостоверяющий центр вправе требовать от заявителя предоставления дополнительных сведений, определенных регламентами и актами владельцев информационных систем, в которых будет использоваться электронная подпись заявителя.

4.1.3. Форма заявления на выдачу сертификата ключа подписи

Форма заявления на выдачу сертификата ключа подписи доступна по ссылке: http://cilink.ru/docs.

4.2. Обработка заявления на выдачу сертификата

4.2.1. Процедура идентификации и аутентификации

Процедуры идентификации и аутентификации осуществляются в порядке, описанном в п.3.2.

4.2.2. Выдача и отказ в выдаче сертификата

Удостоверяющий центр выдает сертификат в случае успешного прохождения заявителем процедур идентификации и аутентификации, описанных в п.3.2.

Удостоверяющий центр вправе отказать заявителю в выдаче сертификата в случае невозможности подтверждения сведений, указанных в заявлении.

4.2.3. Сроки рассмотрения заявления на выдачу сертификата

Удостоверяющий центр обрабатывает заявления в коммерчески оправданные сроки. Как правило, срок обработки заявления не превышает одного рабочего дня. Время выдачи сертификата как правило не превышает 15 минут.

4.3. Изготовление сертификата

4.3.1. Действия удостоверяющего центра при изготовлении сертификата

Сертификат изготавливается оператором удостоверяющего центра в соответствии со сведениями, указанными в заявлении.

4.3.2. Уведомление заявителя о факте изготовления сертификата ключа подписи

Официальным уведомлением пользователей удостоверяющего центра о выдаче сертификата является его публикация в реестре выданных сертификатов.

4.4. Акцепт (признание) сертификата

4.4.1. Действия владельца сертификата, означающие акцепт сертификата

Акцептом сертификата является его первое использование с целью подписания электронного документа.

4.4.2. Публикация сертификата

Удостоверяющий центр публикует реестр выданных сертификатов в соответствии с настоящим регламентом.

4.4.3. Уведомление участников электронного взаимодействия о выдаче сертификата

Официальным уведомлением пользователей удостоверяющего центра о выдаче сертификата ключа подписи является его публикация в реестре выданных сертификатов.

4.5. Использование ключей электронной подписи и сертификатов

4.5.1. Использование ключа электронной подписи и сертификата их владельцем

Допускается использование сертификата строго в соответствии с указанными в нем сведениями.

4.5.2. Использование ключа проверки электронной подписи и сертификата участниками электронного взаимодействия

Участник электронного взаимодействия должен использовать сертификат строго в соответствии с настоящим регламентом и сведениями, указанными в этом сертификате.

Получение дополнительных сведений и гарантий помимо указанных в сертификате осуществляется участником электронного взаимодействия самостоятельно по необходимости.

До принятия решения о доверии к сертификату и/или электронной подписи, участник электронного взаимодействия должен проверить:
- допустимость использования сертификата в соответствии со сведениями об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическую силу;
- сведения о статусе сертификата (проверка факта аннулирования);
- в тех случаях, когда сертификат отозван (аннулирован), или информацию о его статусе получить невозможно, участник электронного взаимодействия должен самостоятельно принять решение об использовании такого сертификата; в этом случае все риски, связанные с доверием к такому сертификату несет участник электронного взаимодействия.

4.6. Обновление сертификата

Обновление сертификата – процедура выдачи сертификата без изменения ключа электронной подписи и сведений, указанных в сертификате.

В настоящее время указанная процедура не осуществляется.

4.7. Смена ключей электронной подписи

Данная процедура подразумевает изготовление новых ключей электронной подписи и ежегодно выполняется удостоверяющим центром для всех владельцев сертификатов.

4.8. Изменение сведений, указанных в сертификате ключа подписи

Процедура подачи заявления и выдачи сертификата при изменении сведений, указанных в сертификате, полностью аналогична процедурам подачи заявления на выдачу сертификата и его обработки, за тем исключением, что заявление на изменение сведений, указанных в сертификате может быть подано в электронном виде и заверено действительной электронной подписью заявителя.

4.9. Отзыв и приостановление действия сертификата

4.9.1. Условия отзыва сертификата

Удостоверяющий центр может отозвать сертификат и осуществить публикацию его в списке отозванных сертификатов в следующих случаях:
- получение от владельца сертификата заявления на отзыв сертификата;
- в удостоверяющий центр представлены доказательства нарушения владельцем сертификата условий настоящего регламента или обязательств перед другими участниками информационных систем;
- прекращение действия соглашения с владельцем сертификата;
- изменение сведений, указанных в сертификате.

4.9.2. Лица, уполномоченные подавать заявления на отзыв сертификатов

Заявление на отзыв сертификата может подавать только его владелец, удостоверяющие центры и центры регистрации, участвовавшие в процессе обработки заявлений на выдачу этих сертификатов, а в случае принадлежности сертификата сотруднику юридического лица – лицо, уполномоченное руководителем организации в соответствии с законодательством.

4.9.3. Процедура подачи заявления на отзыв сертификата

Владелец сертификата обращается в удостоверяющий центр или центр регистрации с письменным заявлением об отзыве сертификата с указанием причины отзыва.

4.9.4. Форма заявления на отзыв сертификата

Заявление на отзыв сертификата подается в письменном виде в произвольной форме с обязательным указанием реквизитов основного документа, удостоверяющего личность заявителя, владельца сертификата, а так же причины отзыва.

4.9.5. Срок подачи заявления на отзыв сертификата

Нет условий.

4.9.6. Срок обработки заявления на отзыв сертификата

Удостоверяющий центр прилагает коммерчески оправданные усилия для скорейшей обработки заявлений на отзыв сертификатов и публикации информации об отзыве этих сертификатов.

4.9.7. Требования к осуществлению проверки факта отзыва сертификата

Участник электронного взаимодействия должен проверять факт отзыва сертификата, полагаясь на достоверность которого он собирается действовать. Проверка факта отзыва может осуществляться с использованием списков отозванных сертификатов или сервиса онлайновой проверки статуса сертификатов, сведения о порядке доступа к которым указаны в проверяемом сертификате.

4.9.8. Частота выпуска списков отозванных сертификатов

Списки отозванных сертификатов публикуются не реже одного раза в сутки.

Сертификаты с истекшим сроком действия, как правило, удаляются из списков отозванных сертификатов.

4.9.9. Задержка публикации списков отозванных сертификатов

Информация об отзыве сертификата ключа подписи публикуется, как правило, в течение нескольких минут после отзыва.

4.9.10. Возможность онлайновой проверки статуса сертификата

Информацию о статусе сертификата можно получить по протоколу онлайновой проверки статуса сертификата. Сведения о порядке доступа к сервису онлайновой проверки статуса сертификата включаются в выдаваемые сертификаты ключей подписей.

4.9.11. Требования к осуществлению онлайновой проверки факта отзыва сертификата

Участник электронного взаимодействия должен самостоятельно осуществлять проверку статуса сертификата ключа подписи, полагаясь на достоверность которого он собирается действовать. В тех случаях, когда для определения степени доверия к сертификату недостаточно использования списков отозванных сертификатов, пользователь должен использовать сервис онлайновой проверки статуса сертификата.

В большинстве случаев рекомендуемые удостоверяющим центром для использования сертифицированные средства электронной цифровой подписи осуществляют вышеуказанные проверки автоматически.

4.9.12. Другие способы извещения участников информационных систем о фактах отзыва сертификатов

Нет условий.

4.9.13. Особые требования в случае компрометации ключей

Удостоверяющий центр прилагает коммерчески оправданные усилия для оповещения участников информационных систем в случае компрометации ключей уполномоченных лиц удостоверяющего центра.

4.9.14. Условия приостановления действия сертификата

Нет условий.

4.9.15. Лица, уполномоченные подавать заявления на приостановление действия сертификатов

Нет условий.

4.9.16. Процедура подачи заявления на приостановление действия сертификата

Удостоверяющий центр производит процедуры отзыва / приостановления сертификата на основании письменного заявления владельца сертификата в соответствии с условиями публичного договора о предоставлении услуг удостоверяющего центра, опубликованном по адресу: http://cilink.ru/docs.

4.9.17. Ограничение срока приостановления действия сертификата

Нет условий.

4.10. Сервис онлайновой проверки статуса сертификата

4.10.1. Рабочие характеристики

Информация о статусах сертификатов доступна с использованием списков отозванных сертификатов и сервиса онлайновой проверки статуса сертификата.

4.10.2. Доступность службы проверки статусов сертификатов

Информация о статусах сертификатов доступна постоянно за исключением запланированных перерывов в работе, сведения о которых публикуются на сайте удостоверяющего центра.

4.10.3. Дополнительные возможности

Нет условий.

4.11. Окончание пользования услугами удостоверяющего центра

Участник электронного взаимодействия может прекратить пользование услугами удостоверяющего центра путем расторжения соглашения о присоединении, путем отзыва своего сертификата(ов) или отказа от смены ключей после окончания их срока действия, при этом он не освобождается от ранее взятых на себя обязательствах перед удостоверяющим центром и другими участниками электронного взаимодействия.

4.12. Депонирование и восстановление ключей

Удостоверяющий центр осуществляет депонирование ключей электронной подписи владельцев сертификатов в специально оборудованных центрах обработки данных, соответствующих промышленным стандартам безопасности.

5. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Для обеспечения безопасности удостоверяющего центра применяются приведенные ниже меры, включающие в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а так же установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

Защита информации от несанкционированного доступа осуществляется на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита информации от несанкционированного доступа предусматривает контроль эффективности средств защиты от несанкционированного доступа. Этот контроль периодически выполняется администраторами безопасности на основе требований документации на средства защиты от несанкционированного доступа.

5.1. Физические меры обеспечения безопасности

5.1.1. Здания и сооружения

Удостоверяющий центр расположен таким образом, чтобы свести к минимуму возможность несанкционированного доступа, аварий и влияние природных явлений.

5.1.2. Физический доступ

Помещения удостоверяющего центра расположены в отдельно стоящем бетонном здании. Все помещения оборудованы системой контроля и управления доступом с идентификацией по смарт-картам, исполнительными устройствами системы контроля доступа электромеханического типа, системой видеонаблюдения.

Серверное оборудование размещается в центрах обработки данных и серверных помещениях, соответствующих требованиям действующего законодательства, предъявляемым к обеспечению безопасности удостоверяющих центров.

Помещения удостоверяющего центра круглосуточно находятся под охраной специализированной организации.

Идентификационные карты для доступа в помещения УЦ выдаются сотрудникам по распоряжению уполномоченного лица удостоверяющего центра.

Посетители допускаются в помещения удостоверяющего центра только в назначенное им время в сопровождении персонала удостоверяющего центра после регистрации в специальных журналах учета посетителей и получения разового пропуска.

5.1.3. Электроснабжение и кондиционирование воздуха

Технические средства удостоверяющего центра подключены к общегородской сети электроснабжения с использованием оборудования бесперебойного питания.

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

Помещения удостоверяющего центра оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

5.1.4. Подверженность воздействию влаги

Защита оборудования удостоверяющего центра от влаги обеспечивается его размещением в специальных серверных шкафах.

5.1.5. Предупреждение и защита от возгорания

Помещения удостоверяющего центра оборудованы средствами пожаротушения в соответствии с требованиями, установленными законодательством Российской федерации.

5.1.6. Хранение архивных документов и электронных носителей

Документальный фонд удостоверяющего центра, как фондообразователя, хранится в соответствии с действующим законодательством по делопроизводству и архивному делу.

5.1.7. Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками удостоверяющего центра, обеспечивающими документирование.

Важные документы и материалы подвергаются уничтожению в специальном оборудовании перед выбрасыванием.

5.1.8. Резервная площадка

Помимо основного центра обработки данных, расположенного в г. Санкт-Петербурге, удостоверяющий центр имеет резервную площадку, расположенную в г. Москве, позволяющую перейти в режим основной в течение 30 минут.

5.2. Организационные меры обеспечения безопасности

5.2.1. Разграничение ролей (полномочий)

Среди сотрудников удостоверяющего центра выделены роли администратора, оператора, аудитора и системного администратора.

Администратор удостоверяющего центра осуществляет:
- управление деятельностью удостоверяющего центра и координация деятельности остальных служб;
- взаимодействие с участниками информационных систем в части разрешения вопросов, связанных с применением средств электронной цифровой подписи, ключей и сертификатов ключей подписей, изготавливаемых и распространяемых удостоверяющим центром;
- взаимодействие с участниками информационных систем в части разрешения вопросов, связанных с подтверждением электронной цифровой подписи уполномоченного лица удостоверяющего центра в сертификатах ключей подписей, изготовленных удостоверяющим центром в электронной форме, или подтверждения собственноручной подписи уполномоченного лица удостоверяющего центра в сертификатах открытых ключей, изготовленных удостоверяющим центром на бумажном носителе.

Оператор УЦ осуществляет:
- регистрацию заявлений;
- ведение реестра абонентов;
- распространение средств ЭЦП;
- изготовление криптографических ключей;
- изготовление и предоставление изготовленных сертификатов ключей подписей в электронной форме по обращению участников информационных систем;
- изготовление и предоставление сертификатов ключей подписей на бумажном носителе по обращению их владельцев;
- аннулирование (отзыв) сертификатов ключей подписей по обращениям их владельцев;
- предоставление участникам информационных систем сведений об аннулированных сертификатах ключей подписей;
- предоставление участникам информационных систем сертификатов ключей подписей, находящихся в реестре изготовленных сертификатов;
- техническое обеспечение процедуры подтверждения электронной цифровой подписи в документах, представленных в электронной форме, по обращениям участников информационных систем;
- техническое обеспечение процедуры подтверждения подлинности электронной цифровой подписи уполномоченного лица удостоверяющего центра, в изготовленных сертификатах открытых ключей, по обращениям участников информационных систем.

Системный администратор удостоверяющего центра осуществляет:
- организацию и выполнению мероприятий по эксплуатации программных и технических средств обеспечения деятельности удостоверяющего центра;

Аудитор осуществляет внутренний аудит деятельности УЦ.

5.3. Требования к персоналу

5.3.1. Квалификации персонала

Сотрудники удостоверяющего центра имеют высшее профессиональное образование, опыт работы в области информационной безопасности более 3 лет.

5.3.2. Проверка биографии сотрудников

Проверка биографии сотрудников осуществляется в соответствии с внутренними инструкциями службы персонала удостоверяющего центра.

5.3.3. Требования к повышению квалификации персонала

Сотрудники удостоверяющего центра проходят курсы повышения квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 2 года.

5.3.4. Требования к повторному прохождению обучения

В случае переноса средств удостоверяющего центра на новое оборудования или программное обеспечение, персонал удостоверяющего центра проходит курс обучения работе с новыми средствами.

5.3.5. Частота и последовательность смены деятельности сотрудников

Нет условий.

5.3.6. Ответственность за нарушения

Персонал удостоверяющего центра несет ответственность за свои действия в соответствии с законодательством РФ.

5.3.7. Требования к независимым подрядчикам

В случаях, когда для выполнения работ требуются услуги независимых подрядчиков, специалисты подрядчиков проводят работы только под наблюдением сотрудников удостоверяющего центра.

5.3.8. Документационное обеспечение персонала

Деятельность сотрудников удостоверяющего центра регламентирована внутренними инструкциями удостоверяющего центра.

Доступ сотрудников удостоверяющего центра к документам и документации, составляющей документальный фонд удостоверяющего центра, организован в соответствии с должностными инструкциями и функциональными обязанностями.

5.4. Порядок ведения записей аудита

5.4.1. Типы событий, подлежащих аудиту

Программно-аппаратный комплекс УЦ регистрирует следующие виды событий:

- системные события общесистемного программного обеспечения;

- принятие запроса на выпуск сертификат открытого ключа;

- выпуск сертификата открытого ключа;

- невыполнение внутренней операции программной компоненты;

- помещение запроса на сертификат;

- принятие запроса на сертификат;

- отклонение запроса на сертификат;

- выпуск списка отозванных сертификатов;

- невыполнение внутренней операции программной компоненты.

Структуры записей событий соответствуют эксплуатационной документации программного обеспечения реализации целевых функций удостоверяющего центра и общесистемного программного обеспечения.

5.4.2. Частота анализа журналов аудита

Журналы аудита еженедельно анализируются с целью обнаружения нарушений в работе программного и аппаратного обеспечения удостоверяющего центра, и анализа производительности систем.

В процессе анализа журналов аудита проводится расследование всех значительных нарушений работы и принимаются адекватные меры реагирования, которые в последствии документируются.

5.4.3. Срок хранения журналов аудита

Журналы аудита подлежат архивированию по истечении двух месяцев после окончания их анализа.

5.4.4. Защита журналов аудита

Журналы аудита защищены от просмотра, модификации и удаления средствами прикладного и общесистемного программного обеспечения.

5.4.5. Резервное копирование журналов аудита

Журналы аудита подлежат инкрементальному резервному копированию ежедневно и полному резервному копированию еженедельно.

5.4.6. Условия сбора записей аудита

События аудита автоматически записываются в журналы средствами прикладного и общесистемного программного обеспечения.

5.4.7. Уведомление субъекта события, вносимого в журнал аудита.

При записи события в журнал аудита, уведомление субъекта этого события не требуется.

5.4.8. Анализ уязвимостей

События, записываемые в журнал аудита, так же служат для анализа уязвимостей удостоверяющего центра. Удостоверяющий центр постоянно проводит анализ уязвимостей и предотвращает их возможные проявления. Все найденные уязвимости и принятые меры по их устранению включаются в ежегодный отчет об аудите.

5.5. Ведение архива

5.5.1. Типы архивных записей

Удостоверяющий центр ведет архив:

- журналов аудита в соответствии с п.5.4;

- соглашений с владельцами сертификатов ключей подписей, договоров и приложений к ним;

- заявлений на выдачу и отзыв сертификатов ключей подписей.

5.5.2. Срок хранения архива

Удостоверяющий центр хранит архив на протяжении всего срока работы.

5.5.3. Защита архива

Удостоверяющий центр обеспечивает хранение архивных документов в соответствии с законодательством РФ.

5.5.4. Резервное копирование архива

Электронные носители архива подлежат инкрементальному резервному копированию ежедневно и полному резервному копированию еженедельно.

5.5.5. Требования к простановке времени создания архивных записей

Нет условий.

5.5.6. Условия архивирования

Удостоверяющий центр обеспечивает ведение архива в соответствии с законодательством РФ.

5.5.7. Порядок получения и проверки информации, хранящейся в архиве

Доступ к архиву имеют только уполномоченные сотрудники удостоверяющего центра. Целостность архива проверяется до извлечения сведений.

5.6. Смена ключей УЦ

Заблаговременно до окончания срока действия ключа подписи уполномоченного лица удостоверяющего центра, администратор удостоверяющего центра производит формирование нового ключа подписи и сертификата уполномоченного лица удостоверяющего центра.

Сформированный новый сертификат записывается в специализированное хранилище, размещенное в центре обработки данных.

По окончании срока действия ключа, отчуждаемые ключевые носители с закрытым ключом, а в случае депонирования ключей в специализированных хранилищах – все экземпляры соответствующих криптоконтейнеров, уничтожаются комиссией с составлением акта уничтожения криптографических ключей.

5.7. Восстановление в случае компрометации или аварии

5.7.1. Действия по предотвращению компрометации и аварии

Резервные копии данных удостоверяющего центра (реестры выпущенных сертификатов), ключей удостоверяющего центра, документационного обеспечения удостоверяющего центра помещаются в специально предназначенные для этих целей хранилища.

5.7.2. Случаи повреждения оборудования, программных и/или аппаратных сбоев

В случае повреждения оборудования, программных и/или аппаратных сбоев, сведения о происшествии поступают в службу безопасности удостоверяющего центра, которая доводит эти сведений до руководства удостоверяющего центра, расследует происшествие и принимает необходимые меры по устранению последствий и недопущению повторения подобных инцидентов.

5.7.3. Компрометация ключа участника информационной системы

К событиям, связанным с компрометацией, относятся следующие события:
- потеря отчуждаемых ключевых носителей, в том числе с их последующим обнаружением;
- увольнение по любой причине сотрудников, имеющих доступ к ключевым носителям или к ключевой информации на данных носителях (возможность такого доступа определяется в зависимости от конкретной реализации системы с СКЗИ и от технологии обработки информации данной системой);
- возникновение подозрений об утечке информации или ее искажении в системе;
- нарушение целостности печати на сейфе с ключевыми носителями или утрата контроля за ключом от такого сейфа;
- утрата пользователем контроля за ограничением доступа к ключевому носителю в процессе эксплуатации им системы;
- случаи, когда невозможно достоверно установить, что произошло с ключевым носителем (например, его разрушение и невозможность опровергнуть подозрение на то, что разрушение носителя произошло не в результате попытки доступа к нему злоумышленника);
- другие виды разглашения ключевой информации, в результате которых закрытые ключи могут стать доступными несанкционированным лицам и (или) процессам.

В случае получения удостоверяющим центром информации о компрометации ключа от его владельца, служба безопасности, абонентский и технический отделы проводят расследование происшествия и принимают необходимые меры в соответствии с указаниями руководства удостоверяющего центра.

В случае необходимости отзыва (аннулирования) сертификата выполняется следующая процедура:
- сведения об аннулировании сертификата в связи с компрометацией доводятся до других участников информационных систем путем публикации в списке отозванных сертификатов;
- владелец скомпрометированного ключа письменно уведомляет других участников информационных систем о факте компрометации в случае необходимости;

- владелец скомпрометированного ключа получает новые ключи и сертификат в порядке, указанном в настоящем регламенте.

5.7.4. Восстановление работоспособности после аварии

План восстановления работоспособности после аварии предполагает восстановление в течение от 24 до 48 часов следующих функций:
- выпуск сертификатов;
- отзыв сертификатов;
- служба онлайновой проверки статусов сертификатов (OCSP);
- служба штампов времени (TSP).

Публикация списков отозванных сертификатов осуществляется непрерывно.

5.8. Разрешение конфликтных ситуаций

5.8.1. Некорректность входящего электронного документа или электронной цифровой подписи

Действия сторон в данной ситуации заключаются в следующем:

Принимающая сторона по телефону (или иным образом) запрашивает у отправляющей стороны информацию о документе, подлинность которого вызывает сомнения. При получении подтверждения об отправке указанного документа, запрашивает повторное оформление и отправку данного документа.

Результатом повторной обработки принимающей стороной (проверка электронной цифровой подписи) полученного документа может быть:

1. Повторная проверка дала отрицательный результат. Подпись документа неверна.

В этом случае делается вывод о возможном нарушении действующего криптографического ключа, либо о неисправности программно-аппаратных средств одной из сторон.

При этом необходимо:

- проверить сертификаты открытых ключей;

- штатными средствами в соответствии с эксплуатационной документацией проверить целостность и неизменность программного обеспечения СКЗИ и СЭП. И переустановить его в случае необходимости.

Если положительного результата достигнуть не удалось, то необходимо обратиться в удостоверяющий центр.

2. Повторная проверка дала положительный результат. Подпись документа верна.

5.8.2. Непризнание отправителем электронного документа факта отправки документа, а также его целостности и подлинности

В случае если одна из сторон приходит к выводу, что другая сторона ссылается на документ, исходящий от первой, который не отправлялся и/или его содержание изменено, следует известить удостоверяющий центр о наличии конфликтной ситуации.

Удостоверяющий центр формирует Экспертную (согласительную) комиссию для разрешения конфликтной ситуации, в состав которой входят представители участников, вовлеченных в конфликтную ситуацию. Дополнительно могут привлекаться авторитетные, независимые специалисты в области криптографической защиты информации.

В ходе работы Экспертной комиссии рассматриваются документы, в том числе электронные, относящиеся к предмету разногласий, и выполняется процедура проверки ЭЦП документа. При этом могут быть использованы следующие эталонные данные:

- данные архива оригиналов принятых/отправленных документов;

- сертификаты ключей подписей, выданные Удостоверяющим Центром;

- дистрибутивы СКЗИ;

- ключевые носители.

Процедура проверки ЭП документа
Для проведения разбора конфликтной ситуации необходимы:

- заверенный удостоверяющим центром сертификат пользователя, подписавшего документ, подлинность или авторство которого оспаривается.

- файл, содержащий текст документа и электронную цифровую подпись его автора, в отношении которого возникает конфликтная ситуация.

Для разбора конфликтной ситуации необходимо выполнить следующие действия:

Произвести операцию проверки подписи электронного документа, авторство подписи которого оспаривается на рабочем месте администратора УЦ (АРМ Разбора конфликтных ситуаций).

Распечатать протокол проверки подписи.

Распечатать сертификат из Реестра удостоверяющего центра.

Сравнить представленный сертификат и распечатанный сертификат из Реестра удостоверяющего центра.

Авторство подписи под документом считается установленным, если совпадают открытые ключи представленного сертификата и сертификат из Реестра удостоверяющего центра, и в протоколе проверки подписи пользователя сформирована запись «Подпись верна».

5.9. Прекращение работы удостоверяющего центра

В случае прекращения работы, удостоверяющий центр принимает все меры по минимизации влияния указанного процесса на участников информационных систем в соответствии с действующим законодательством.

6. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

6.1. Изготовление и установка ключевой пары

6.1.1. Изготовление ключей

Изготовление ключей проводится удостоверяющим центром.

В качестве ключевого носителя используются сертифицированные СКЗИ, отчуждаемые ключевые носители, совместимые с указанными СКЗИ, либо специализированные хранилища (HSM – англ. hardware security module - аппаратный модуль безопасности), с помощью которых производится изготовление ключей.

6.1.2. Передача ключа подписи владельцу

Нет условий.

6.1.3. Передача ключа проверки подписи в удостоверяющий центр

Нет условий.

6.1.4. Передача ключей проверки подписей участникам электронного взаимодействия

Удостоверяющий центр публикует сертификаты, содержащие ключи проверки подписей их владельцев и списки отозванных сертификатов в соответствии с порядком, описанном в настоящем регламенте.

Сведения о публикации сертификатов уполномоченных лиц удостоверяющего центра содержатся в каждом выданном сертификате. Цепочки доверия, как правило, строятся программным обеспечением автоматически.

До начала использования сертификата участник электронного взаимодействия должен установить доверие к сертификатам уполномоченных лиц удостоверяющего центра в своей системе.

Скачав и установив сертификаты уполномоченных лиц удостоверяющего центра, пользователь подтверждает свое присоединение к настоящему регламенту и полное и безоговорочное согласие с условиями использования сервисов удостоверяющего центра.

6.1.5. Размеры ключей

Размеры ключей электронной цифровой подписи устанавливаются государственными стандартами РФ.

6.1.6. Параметры генерации и проверки качества ключа подписи

Определяются сертифицированным СКЗИ и СЭП автоматически.

6.1.7. Цели использования ключа подписи (порядок заполнения поля key usage сертификата x.509v3)

Заполняются в соответствии с назначением сертификата и требованиями информационных систем, в которых указанные сертификаты будут использоваться.

6.2. Защита ключа подписи, требования к ключевым носителям и криптографическим модулям

Все действия с ключевыми носителями должны осуществляться строго в соответствии с инструкциями по их эксплуатации и требованиями безопасности.

6.2.1. Требования к ключевым носителям

Нет условий.

6.2.2. Ключ подписи, контролируемый несколькими держателями (n из m)

Нет условий.

6.2.3. Депонирование ключей подписи

Удостоверяющий центр может депонировать ключи подписи с использованием сертифицированных СКЗИ и / или в специализированном промышленном хранилище (HSM). Доступ владельцев к ключам подписи осуществляется с использованием кодов и паролей.

6.2.4. Резервное копирование ключа подписи

Нет условий.

6.2.5. Архивирование ключа подписи

Ключи подписи с истекшим сроком действия подлежат уничтожению в соответствии с эксплуатационной документацией средства криптографической защиты информации. Архивное хранение закрытых ключей не допускается.

6.2.6. Запись ключа подписи в криптографический модуль

Производится автоматически средствами средства криптографической защиты информации в соответствии с эксплуатационной документацией.

6.2.7. Хранение ключа подписи в криптографическом модуле

Ключи подписи хранятся только в зашифрованном виде.

6.2.8. Способы активации ключа подписи

Активация ключа подписи происходит при подключении специализированного устройства и/или ввода кода (пароля) доступа к ключам электронной подписи, передаваемого клиенту после подписания заявления о выдаче сертификата, к персональному компьютеру с установленным необходимым для работы программным обеспечением. Специализированное устройство содержит необходимые коды доступа к ключам подписи.

6.2.9. Способы деактивации ключа подписи

Ключ подписи деактивируется средством криптографической защиты информации автоматически после выполнения связанных с его использованием операций или после физического отключения специализированного устройства доступа от персонального компьютера.

6.2.10. Способы уничтожения ключа подписи

Уничтожение ключа подписи производится в соответствии с эксплуатационной документацией средства криптографической защиты информации.

6.2.11. Оценка криптографического модуля

Криптографические модули, используемые удостоверяющим центром, соответствуют промышленным стандартам и законодательству в области безопасности.

6.3. Другие особенности использования ключей подписи

6.3.1. Архивирование ключей проверки подписи

Все сертификаты ключей проверки подписи архивируются в соответствии с порядком резервного копирования, установленным в удостоверяющем центре.

6.3.2. Сроки действия сертификатов и ключей

Срок действия ключа подписи уполномоченного лица удостоверяющего центра составляет 3 года. В течение 1 года 3 месяцев с момента начала срока действия ключа подписи уполномоченного лица удостоверяющего центра, ключ подписи используется для изготовления сертификатов и формирования списков отозванных сертификатов. По истечении 1 года 3 месяцев и до окончания срока действия ключа подписи уполномоченного лица удостоверяющего центра, данный ключ используется исключительно для формирования списков отозванных сертификатов. Срок действия сертификата уполномоченного лица удостоверяющего центра составляет 30 лет.

Сроки действия сертификатов сервисов актуальных статусов сертификатов и штампов времени составляют 25 лет.

Сроки действия ключей подписи и сертификатов участников электронного взаимодействия составляет 1 год.

6.4. Данные активации ключей подписи

6.4.1. Генерация и установка данных активации ключа подписи

Данные активации, предназначенные для защиты ключей, устанавливаются системным программным обеспечением специализированного ключевого хранилища.

6.4.2. Защита данных активации ключа подписи

Запрещается передавать устройство доступа со встроенным модулем идентификации (или карты с модулем идентификации), полученное клиентом при подаче заявления на выдачу сертификата, коды доступа и пароли к ключам подписи.

6.4.3. Особенности данных активации закрытого ключа

Нет условий.

6.5. Меры обеспечения информационной безопасности

Удостоверяющий центр имеет аттестаты соответствия требованиям по классу защищенности 1Г РД ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Все участники электронного взаимодействия, использующие услуги удостоверяющего центра должны осуществлять эксплуатацию средств электронной цифровой подписи строго в соответствии с эксплуатационной документацией.

7. ПРОФИЛИ СЕРТИФИКАТОВ И CRL

7.1. Профиль сертификата

7.1.1. Версия сертификата

Удостоверяющий центр выдает сертификаты в электронной форме формата X.509 версии 3.

7.1.2. Расширения сертификата

Сертификаты содержат следующие дополнения:

authorityKeyIdentifier	Идентификатор ключа уполномоченного лица УЦ
subjectKeyIdentifier	Идентификатор ключа владельца сертификата
ExtendedKeyUsage	Область (области) использования ключа, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) сертификатов
FreshestCRL	Точка распространения delta-CRL
KeyUsage	Назначение ключа

7.1.3. Объектные идентификаторы алгоритмов

Удостоверяющий центр использует следующие идентификаторы алгоритмов средства электронной цифровой подписи:

ГОСТ Р 34.10-2001	1.2.643.2.2.19
ГОСТ Р 34.11-94	1.2.643.2.2.9
ГОСТ 28147-89	1.2.643.2.2.21
Диффи-Хеллмана	1.2.643.2.2.98
RSA with SHA1	1.3.14.3.2.29
SHA1	1.3.14.3.2.26

7.1.4. Форматы имен (идентификационных данных)

В сертификатах поля идентификационных данных уполномоченного лица УЦ и владельца сертификата содержат атрибуты имени в формате X.500.

Сертификаты содержат следующие базовые поля X.509:

Signature:	Электронная подпись уполномоченного лица УЦ
Issuer:	Идентифицирующие данные уполномоченного лица УЦ
Validity:	Даты начала и окончания срока действия сертификата
Subject:	Идентифицирующие данные владельца сертификата
SubjectPublicKeyInformation:	Идентификатор алгоритма средства электронной подписи, с которыми используется данный открытый ключ, значение открытого ключа
Version:	Версия сертификата формата X.509 - версия 3

SerialNumber:	Уникальный серийный (регистрационный) номер сертификата в реестре сертификатов УЦ

Обязательными атрибутами поля идентификационных данных уполномоченного лица УЦ являются:

Common Name	Фамилия, имя, отчество или Псевдоним
Organization	Наименование организации, являющейся владельцем УЦ
Email	Адрес электронной почты
Country	RU

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

Common Name	Номер контракта, заключенного с удостоверяющим центром, однозначно идентифицирующий владельца сертификата
Country	RU

7.1.5. Ограничения, накладываемые на имена (идентификационные данные)

На идентификационные данные налагаются ограничения по содержанию, длинам строк и используемым символам в соответствии с x.500.

7.1.6. Объектный идентификатор политики сертификата

Нет условий.

7.1.7. Использование расширения Policy Constraints

Нет условий.

7.1.8. Использование расширения Policy Qualifier

Нет условий.

7.1.9. Порядок обработки расширений Certificate Policies, имеющих пометку critical.

Решение о доверии к сертификату принимается участником электронного взаимодействия самостоятельно.

7.2. Профиль CRL

Удостоверяющий центр формирует списки отозванных сертификатов в электронной форме (CRL, COC) формата X.509 версии 2.

7.3. Дополнения CRL

Удостоверяющий центр использует следующие дополнения:

Authority Key Identifier	Идентификатор ключа уполномоченного лица УЦ
Reason Code	Код причины отзыва сертификата открытого ключа