

УТВЕРЖДАЮ

Заместитель министра информационной
политики и массовых коммуникаций
Чувашской Республики

 А. Н. Сидоренко



20 16 г.

РЕГЛАМЕНТ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
МИНИСТЕРСТВА
ИНФОРМАЦИОННОЙ ПОЛИТИКИ И
МАССОВЫХ КОММУНИКАЦИЙ
ЧУВАШСКОЙ РЕСПУБЛИКИ

1. Сведения об Удостоверяющем центре.

Министерство информационной политики и массовых коммуникаций Чувашской Республики (далее также – Министерство) выполняет функции удостоверяющего центра в соответствии Федеральным Законом «Об электронной подписи» и Положением о Министерстве информационной политики и массовых коммуникаций Чувашской Республики, утвержденным постановлением Кабинета Министров Чувашской Республики от 06 июня 2012 г. № 218.

В соответствии с Указом Главы Чувашской Республики от 25 мая 2012 г. № 49 «О мерах по совершенствованию государственного управления Чувашской Республики» Государственный комитет Чувашской Республики по связи и информатизации преобразован в Министерство информационной политики и массовых коммуникаций Чувашской Республики, которое является правопреемником по обязательствам Государственного комитета Чувашской Республики по связи и информатизации и имеет разрешение (лицензии) по всем видам деятельности, связанных с выполнением функций удостоверяющего центра (далее также – УЦ).

Реквизиты Мининформполитики Чувашии:

Полное наименование юридического лица: Министерство информационной политики и массовых коммуникаций Чувашской Республики.

Сокращенное наименование юридического лица: Мининформполитики Чувашии.

Юридический адрес: 428004, г.Чебоксары, Президентский бульвар, д.10

Фактическое местонахождение: 428004, г.Чебоксары, Президентский бульвар, 10

ОГРН: 1122130008791

ИНН/КПП: 2130106185/213001001

Свидетельство о государственной регистрации юридического лица от 20 июля 2012 года №002302456, выдано Инспекцией Федеральной налоговой службы по г.Чебоксары.

Свидетельство о постановке на учет в налоговом органе от 20 июля 2012 года №002302712, выдано Инспекцией Федеральной налоговой службы по г.Чебоксары.

л/с: 03262403791 в УФК по Чувашской Республике

р/с: 40201810300000100004 в ГРКЦ НБ Чувашской Республики Банка России
г.Чебоксары

БИК: 049706001

ОКПО: 71011036

ОКАТО: 97401368000

ОКВЭД-2001: 75.11.21

Контактные телефоны, адрес электронной почты:

Телефон: (8352) 64-20-90; Факс: (8352)64-20-96; e-mail: info100@cap.ru

Контактные телефоны, адрес электронной почты Уполномоченного лица УЦ:

Телефон: (8352) 64-20-92; e-mail: certadmin@cap.ru.

Адрес сайта Мининформполитики Чувашии: <http://www.info.cap.ru>

Адрес сайта УЦ: <http://uc.cap.ru/>; <http://www.cap.ru/certsrv>

2. Термины и определения.

2.1. **Аутентификация** – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности электронной подписи.

2.2. **Владелец сертификата ключа проверки электронной подписи** (далее также - Владелец сертификата) – лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке и в соответствии с настоящим Регламентом выдан сертификат ключа проверки электронной подписи.

2.3. **Доверенное лицо Клиента** – физическое лицо, действующее от имени юридического лица, уполномоченное на предоставление документов для изготовления и получения сертификатов ключей проверки электронной подписи и средств электронной подписи.

2.4. **Доверенное лицо Удостоверяющего центра** – физическое лицо или юридическое лицо, наделенное Министерством полномочиями по созданию и выдаче сертификатов ключей проверки электронной подписи, а также иными полномочиями согласно настоящему Регламенту.

2.5. **Запрос на отзыв сертификата** – электронный документ, содержащий необходимую информацию для отзыва сертификата.

2.6. **Запрос на сертификат** – электронный документ, содержащий необходимую информацию для изготовления сертификата.

2.7. **Заявитель** – юридическое лицо, являющееся Участником электронного взаимодействия органов государственной власти Чувашской Республики и обращающиеся в Удостоверяющий центр для регистрации юридического лица, Уполномоченного представителя юридического лица или должностного лица Заявителя в Удостоверяющем центре качестве Пользователя Удостоверяющего центра, получения средства электронной подписи и сертификата ключа проверки электронной подписи.

2.8. **Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

2.9. **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.

2.10. **Клиент Удостоверяющего центра** (далее также – Клиент) – юридическое лицо, являющееся Участником электронного взаимодействия и присоединившееся к Регламенту Удостоверяющего центра.

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

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

2.13. **Ключевой носитель** – носитель, предназначенный для хранения и содержащий ключ электронной подписи.

2.14. **Компрометация ключа** – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

2.15. **Корпоративная информационная система** - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

2.16. **Корпоративная информационная система органов государственной власти Чувашской Республики** – информационная система, участниками электронного взаимодействия которой являются органы исполнительной власти Чувашской Республики, органы местного самоуправления в Чувашской Республике, территориальные органы федеральных органов исполнительной власти, иные государственные органы, а также организации, финансируемые из республиканского бюджета Чувашской

Республики и уполномоченные лица участников корпоративной информационной системы органов государственной власти Чувашской Республики.

2.17. Оператор Удостоверяющего центра (далее также – Оператор УЦ) – должностное лицо, наделённое Министерством полномочиями по обслуживанию сертификатов ключей проверки электронной подписи, внесению сведений в реестр сертификатов и иными полномочиями согласно настоящему Регламенту.

2.18. Плановая смена ключей – смена ключей электронной подписи с установленной в системе периодичностью, не вызванная компрометацией ключей.

2.19. Пользователь Удостоверяющего центра (далее также – Пользователь УЦ) – юридическое лицо, Уполномоченный представитель юридического лица или должностное лицо Клиента, являющееся участником электронного взаимодействия корпоративной информационной системы органов государственной власти Чувашской Республики и зарегистрированное в Удостоверяющем центре.

2.20. Рабочее время Удостоверяющего центра (далее – рабочее время) – промежутки времени с 08:00 по 17:00 (время Московское) ежедневно с понедельника по пятницу за исключением выходных и праздничных дней.

2.21. Реестр сертификатов – реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей, включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях прекращения или аннулирования таких сертификатов.

2.22. Сертификат ключа проверки электронной подписи (далее также – сертификат) – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2.23. Список отозванных сертификатов (далее также – СОС) – электронный документ, подписанный электронной подписью уполномоченного лица удостоверяющего центра, содержащий список серийных номеров сертификатов ключей проверки электронной подписи, которые на определенный момент времени были аннулированы или действие которых было приостановлено на основании заявления владельца сертификата.

2.24. Средства удостоверяющего центра (далее также – средства УЦ) – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

2.25. Средства электронной подписи (далее также – 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.

2.26. Уполномоченное лицо Удостоверяющего центра – должностное лицо Министерства, наделенное полномочиями по заверению сертификатов ключей проверки электронной подписи и списков отозванных сертификатов, а также иными полномочиями согласно настоящему Регламенту.

2.27. Уполномоченный представитель юридического лица – физическое лицо, которое действует от имени Заявителя – юридического лица на основании учредительных документов юридического лица или доверенности.

2.28. Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

2.29. Участники электронного взаимодействия органов государственной власти Чувашской Республики – осуществляющие обмен информацией в электронной форме органы исполнительной власти Чувашской Республики, органы местного

самоуправления в Чувашской Республике, территориальные органы федеральных органов исполнительной власти, иные государственные органы, а также организации, финансируемые из республиканского бюджета Чувашской Республики и уполномоченные лица участников электронного взаимодействия органов государственной власти Чувашской Республики.

2.30. Электронный документ (далее также - 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.

2.31. Электронная подпись (далее также - 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.

3. Общие положения.

3.1. Статус Регламента.

3.1.1. Регламент удостоверяющего центра Министерства информационной политики и массовых коммуникаций Чувашской Республики (далее также – Регламент) разработан в соответствии с Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения в области использования электронных подписей.

3.1.2. Настоящий Регламент устанавливает порядок реализации функций, осуществления прав и исполнения обязанностей удостоверяющего центра Министерства информационной политики и массовых коммуникаций Чувашской Республики (далее также – Удостоверяющий центр), порядок и условия предоставления услуг Удостоверяющего центра, а также определяет права и обязанности лиц, присоединившихся к Регламенту.

3.2. Публикация Регламента.

Настоящий Регламент распространяется:

- в электронной форме на сайте УЦ по адресу: <http://www.cap.ru/certsrv/>
- в бумажной форме через почтовый адрес: 428004, Чувашская Республика, г.Чебоксары, Президентский бульвар, д.10, Министерство информационной политики и массовых коммуникаций Чувашской Республики.

3.3. Область применения Регламента.

3.3.1. Настоящий Регламент предназначен служить соглашением, определяющим права, обязанности и ответственность сторон, а также средством официального уведомления и информирования сторон во взаимоотношениях, возникающих в процессе предоставления услуг Удостоверяющего центра.

3.3.2. Сторонами согласно настоящему Регламенту являются Министерство информационной политики и массовых коммуникаций Чувашской Республики и лицо, присоединившиеся к Регламенту.

3.3.3. Стороны обязаны соблюдать требования Федерального закона «Об электронной подписи», других федеральных законов и принимаемых в соответствии с ними нормативных правовых актов, регулирующих отношения в области использования электронных подписей, а также требования настоящего Регламента.

3.4. Присоединение к Регламенту.

3.4.1. Присоединение к настоящему Регламенту осуществляется путем подписания Заявителем надлежащим образом оформленного заявления о присоединении к Регламенту Удостоверяющего центра по форме Приложения № 2 настоящего Регламента.

3.4.2. С момента регистрации в Удостоверяющем центре Заявления о присоединении к Регламенту в Удостоверяющем центре, Заявитель признается Стороной присоединившейся к Регламенту и является Клиентом Удостоверяющего центра.

3.4.3. С момента регистрации Клиента или его Уполномоченного представителя в реестре Удостоверяющего центра, Клиент или его Уполномоченный представитель признается зарегистрированным Пользователем УЦ.

3.4.4. С момента изготовления сертификата ключа проверки электронной подписи зарегистрированного Пользователя УЦ и выдачи его Клиенту или Доверенному лицу Клиента, Пользователь УЦ считается Владельцем сертификата.

3.4.5. Факт присоединения к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент присоединения к Регламенту. Сторона, присоединившаяся к Регламенту, принимает дальнейшие изменения, вносимые в Регламент.

3.5. Порядок расторжения Регламента.

3.5.1. Действие настоящего Регламента может быть прекращено по инициативе одной из Сторон в следующих случаях:

- по собственному желанию одной из Сторон;
- нарушения одной из Сторон условий настоящего Регламента.

3.5.2. В случае расторжения Регламента инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за тридцать календарных дней до даты расторжения Регламента. Регламент считается расторгнутым после выполнения Сторонами своих обязательств.

3.5.3. Прекращение действия Регламента не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

3.6. Утверждение и внесение изменений в Регламент.

3.6.1. Настоящий Регламент составляется в письменной форме и утверждается приказом Министерства информационной политики и массовых коммуникаций Чувашской Республики.

3.6.2. Внесение изменений в Регламент, в том числе приложений к нему, производится Удостоверяющим центром в одностороннем порядке.

3.6.3. Уведомление пользователей УЦ о внесении изменений в Регламент осуществляется Удостоверяющим центром в соответствии с п. 3.2 настоящего Регламента, путем публикации новой версии Регламента, включающего внесенные изменения.

3.6.4. Изменения, вносимые в Регламент, кроме изменений, вызванных в связи с изменениями в нормативных правовых актах, регулирующих отношения в области использования электронных подписей, вступают в силу и становятся обязательными для Сторон по истечению 10 (десяти) календарных дней с даты их публикации.

3.6.5. Изменения, вносимые в Регламент в связи с изменениями в нормативных правовых актах, регулирующих отношения в области использования электронных подписей, вступают в силу одновременно с вступлением в силу изменений в указанных нормативных правовых актах.

3.6.6. С момента вступления в силу изменений, внесенных в Регламент, их действие распространяется на всех лиц, присоединившихся к Регламенту, в том числе лиц, присоединившихся к Регламенту ранее даты вступления изменений в силу.

3.7. Применение Регламента.

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

3.7.2. В случае противоречия или расхождения названия какого-либо раздела Регламента со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

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

4. Предоставление информации.

4.1. Удостоверяющий центр предоставляет Стороне, присоединившейся к Регламенту, по ее требованию:

- копию Регламента удостоверяющего центра Министерства информационной политики и массовых коммуникаций Чувашской Республики;
- копии лицензий ФСБ России на осуществление деятельности по распространению шифровальных (криптографических средств), деятельности по

техническому обслуживанию шифровальных (криптографических средств), деятельности на предоставление услуг в области шифрования информации;

- копию сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра;
- копии сертификатов ключей проверки электронной подписи лиц, зарегистрированных в реестре Удостоверяющего центра.

4.2. Удостоверяющий центр вправе запросить, а Сторона, присоединившаяся к Регламенту, обязана предоставить документы, подтверждающие достоверность информации, предоставленной заявителем, либо их надлежащим образом заверенные копии:

- учредительные документы;
- документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц;
- свидетельство о постановке на учет в налоговом органе;
- доверенность или иной документ, подтверждающий право Заявителя действовать от имени других лиц;
- документ, подтверждающий полномочия лица, обращающегося за получением сертификата, действовать от имени Заявителя - юридического лица;
- основной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования.

5. Деятельность Удостоверяющего центра.

5.1. Назначение Удостоверяющего центра.

5.1.1. Удостоверяющий центр предназначен для обеспечения участников электронного взаимодействия корпоративной информационной системы органов государственной власти Чувашской Республики средствами электронной подписи и сертификатами ключей проверки электронной подписи в целях:

- применения электронной подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе электронного взаимодействия;
- аутентификации участников электронного взаимодействия;
- обеспечения конфиденциальности информации, представленной в электронном виде, передаваемой в процессе электронного взаимодействия.

5.1.2. Участникам электронного взаимодействия корпоративной информационной системы органов государственной власти Чувашской Республики услуги Удостоверяющего центра предоставляются на безвозмездной основе.

5.1.3. Участниками электронного взаимодействия корпоративной информационной системы органов государственной власти Чувашской Республики и пользователями Удостоверяющего центра являются органы исполнительной власти Чувашской Республики, органы местного самоуправления в Чувашской Республике, территориальные органы федеральных органов исполнительной власти, иные государственные органы и их уполномоченные представители, а также организации, финансируемые из республиканского бюджета Чувашской Республики.

5.2. Услуги, предоставляемые Удостоверяющим центром.

5.2.1. Внесение в реестр Удостоверяющего центра регистрационной информации о пользователях УЦ.

5.2.2. Изготовление сертификатов ключей проверки электронной подписи.

5.2.3. Формирование ключей электронной подписи и ключей проверки электронной подписи по обращениям пользователей УЦ с записью их на ключевой носитель.

5.2.4. Ведение реестра изготовленных сертификатов ключей проверки электронной подписи.

5.2.5. Предоставление сертификатов ключей проверки электронной подписи в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ.

5.2.6. Аннулирование (отзыв) сертификатов по обращениям владельцев сертификатов ключей проверки электронной подписи.

5.2.7. Приостановление и возобновление действия сертификатов по обращениям владельцев сертификатов ключей проверки электронной подписи.

5.2.8. Предоставление пользователям УЦ сведений об аннулированных и приостановленных сертификатах.

5.2.9. Подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям пользователей УЦ.

5.2.10. Подтверждение подлинности электронных подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах ключей проверки электронной подписи по обращениям пользователей УЦ.

5.2.11. Предоставление по обращениям пользователей УЦ средств электронной подписи (неисключительной лицензии на право использования средства электронной подписи).

5.2.12. Предоставление пользователям УЦ информации об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

5.2.13. Предоставление любым лицам, обратившимся в УЦ, информации, содержащейся в реестре сертификатов, в том числе информации об аннулировании сертификата ключа проверки электронной подписи.

5.2.14. Предоставление иных услуг, связанных с использованием электронной подписи.

5.3. Прекращение деятельности Удостоверяющего центра.

5.3.1. Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения в области использования электронных подписей.

5.3.2. Министерство, в случае принятия решения о прекращении деятельности УЦ, сообщает об этом в уполномоченный федеральный орган не позднее, чем за один месяц до даты прекращения деятельности УЦ, уведомляет пользователей УЦ, срок действия сертификатов которых не истек, передает в уполномоченный федеральный орган в установленном порядке Реестр сертификатов и подлежащую хранению информацию.

6. Права и обязанности сторон.

6.1. Права Участников электронного взаимодействия.

6.1.1. Получить сертификат Уполномоченного лица Удостоверяющего центра.

6.1.2. Получить сертификат Пользователя УЦ, находящийся в реестре сертификатов Удостоверяющего центра.

6.1.3. Использовать сертификат Пользователя УЦ для проверки электронной подписи.

6.1.4. Использовать списки отозванных сертификатов для проверки действительности сертификатов, созданных и выданных Удостоверяющим центром.

6.1.5. Обратиться в Удостоверяющий центр за проверкой подлинности электронной подписи, сертификат ключа проверки которой был выдан Удостоверяющим центром.

6.2. Обязанности Участников электронного взаимодействия.

6.2.1. Обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия.

6.2.2. Уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

6.2.3. Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

6.2.4. Использовать для создания и проверки электронных подписей, создания ключей электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

6.3. Права Удостоверяющего центра.

6.3.1. Отказать в регистрации в Удостоверяющем центре в случае ненадлежащего оформления необходимых регистрационных документов, указанных в пункте 4.2 Регламента, а также в случае непредставления документов, предоставления документов не в полном объеме или предоставления документов, подлинность которых вызывает сомнение.

6.3.2. Отказать в регистрации или изготовлении сертификата Пользователя УЦ в случае ненадлежащего оформления заявления на регистрацию или заявления изготовления сертификата.

6.3.3. Отказать Пользователю УЦ в изготовлении сертификата в случае, если средство электронной подписи, использованное Пользователем УЦ для формирования запроса на сертификат, не поддерживается Удостоверяющим Центром.

6.3.4. Отказать в аннулировании (отзыве), приостановлении и возобновлении действия сертификата Пользователя УЦ в случае ненадлежащего оформления соответствующего заявления на аннулирование (отзыв), приостановление и возобновление действия сертификата.

6.3.5. Отказать Пользователю УЦ в исполнении услуги аннулирования (отзыва) или приостановления действия сертификата с использованием кодовой фразы в случае невозможности аутентификации Пользователя УЦ по кодовой фразе.

6.3.6. Отказать в отзыве, приостановлении и возобновлении действия сертификата Пользователя УЦ в случае, если истек срок действия ключа электронной подписи, соответствующего сертификату.

6.3.7. В одностороннем порядке приостановить действие сертификата Пользователя УЦ с обязательным уведомлением владельца сертификата, действие которого приостановлено, и указанием обоснованных причин.

6.3.8. Отказать в предоставлении информации, содержащейся в реестре сертификатов, в случае, если объем запрашиваемой информации не соответствует законной цели обработки, заявленной в запросе на предоставление информации.

6.4. Обязанности Удостоверяющего центра.

6.4.1. Оказывать услуги в соответствии с требованиями, устанавливаемыми Федеральным законом «Об электронной подписи», другими федеральными законами и принимаемыми в соответствии с ними нормативными актами.

6.4.2. Использовать средства электронной подписи и средства удостоверяющего центра, получившие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

6.4.3. Предоставить Пользователю УЦ сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра в электронной форме.

6.4.4. Использовать ключ электронной подписи уполномоченного лица Удостоверяющего центра только для подписи издаваемых им сертификатов ключей подписей и списков отозванных сертификатов.

6.4.5. Принять меры по защите ключа электронной подписи уполномоченного лица Удостоверяющего центра от несанкционированного доступа.

6.4.6. Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса по местонахождению Удостоверяющего центра и обеспечить синхронизацию по времени средств удостоверяющего центра.

6.4.7. Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным в настоящем Регламенте.

6.4.8. Обеспечить занесение регистрационной информации Пользователя УЦ в реестр Удостоверяющего центра и обеспечить уникальность регистрационной информации, используемой для идентификации владельцев сертификатов.

6.4.9. Изготовить сертификат ключа проверки электронной подписи Пользователя УЦ по заявлению на изготовление сертификата, в соответствии с порядком, определенным в настоящем Регламенте.

6.4.10. Обеспечить уникальность серийных номеров изготавливаемых сертификатов.

6.4.11. Обеспечить уникальность ключей проверки электронных подписей в реестре сертификатов.

6.4.12. Обеспечить конфиденциальность созданных Удостоверяющим центром ключей электронных подписей в пределах средств, находящихся в зоне ответственности Удостоверяющего центра.

6.4.13. Обеспечить актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

6.4.14. В течение одного рабочего дня внести сведения о выданных сертификатах в реестр сертификатов.

6.4.15. Обеспечить хранение в форме, позволяющей проверить ее целостность и достоверность, в течение срока его деятельности Удостоверяющего центра следующей информации: реквизиты основного документа, удостоверяющего личность владельца сертификата; сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя, обращаться за получением сертификата; сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца сертификата включена в сертификат.

6.4.16. Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.

6.4.17. Обеспечить изготовление ключа электронной подписи Пользователя УЦ средствами электронной подписи, предусматривающими запись ключа электронной подписи непосредственно на ключевой носитель Пользователя УЦ, без сохранения сформированной ключевой информации на каком-либо ином носителе.

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

6.4.19. Аннулировать (отозвать), приостановить и возобновить действие сертификата Пользователя УЦ по соответствующему заявлению на аннулирование (отзыв), приостановление и возобновление действия сертификата, в соответствии с порядком, определенным в настоящем Регламенте.

6.4.20. Аннулировать (отозвать) сертификат Пользователя УЦ, если истек установленный срок, на который действие данного сертификата было приостановлено.

6.4.21. Аннулировать (отозвать) сертификат Пользователя УЦ в случае компрометации ключа электронной подписи уполномоченного лица УЦ, с использованием которого был подписан сертификат Пользователя УЦ.

6.4.22. Официально уведомить всех лиц, зарегистрированных в Удостоверяющем центре, об аннулировании (отзыве), приостановлении и возобновлении действия сертификата Пользователя УЦ путем занесения информации в список отозванных сертификатов.

6.4.23. Публиковать актуальный список отозванных сертификатов на сайте Удостоверяющего центра <http://www.cap.ru/certsrv/> и обеспечить его круглосуточную доступность. Период публикации списка отозванных сертификатов в рабочее время Удостоверяющего центра – 24 часа. Срок публикации списка отозванных сертификатов может изменяться в одностороннем порядке. Точки распространения списка отозванных сертификатов указываются в сертификате Пользователя УЦ.

6.4.24. В случае принятия решения о прекращении своей деятельности, сообщить об этом на сайте Удостоверяющего центра <http://www.cap.ru/certsrv/> и в уполномоченный федеральный орган не позднее, чем за один месяц до даты прекращения своей деятельности, передать в уполномоченный федеральный орган реестр сертификатов и информацию, подлежащую хранению.

6.5. Права Стороны, присоединившейся к Регламенту.

6.5.1. Применять сертификат уполномоченного лица УЦ для проверки электронной подписи уполномоченного лица УЦ в сертификатах, изготовленных Удостоверяющим центром.

6.5.2. Применять список отозванных сертификатов, изготовленный Удостоверяющим центром, для установления статуса сертификатов пользователей УЦ.

6.5.3. Применять сертификат пользователя УЦ для проверки электронной подписи в соответствии со сведениями, указанными в сертификате.

6.5.4. Для хранения ключа электронной подписи применять носитель, поддерживаемый средством электронной подписи.

6.5.5. Обратиться в Удостоверяющий центр с заявлением на изготовление сертификата.

6.5.6. Обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) и приостановление действия сертификата, владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи.

6.5.7. Обратиться в Удостоверяющий центр с заявлением на возобновление действия сертификата, владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи и срока, на который действие сертификата было приостановлено.

6.5.8. Обратиться в Удостоверяющий центр за получением информации о статусе сертификатов и их действительности на определенный момент времени.

6.5.9. Обратиться в Удостоверяющий центр за подтверждением подлинности электронной подписи, сформированной с использованием сертификата, изданного Удостоверяющим центром.

6.5.10. Обратиться в Удостоверяющий центр для получения средств электронной подписи (неисключительной лицензии на право использования средства электронной подписи).

6.5.11. Обратиться в Удостоверяющий центр для получения информации об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

6.6. Обязанности Стороны, присоединившейся к Регламенту.

6.6.1. Представить оригиналы документов, либо их надлежащим образом заверенные копии, подтверждающие достоверность информации, включаемой в сертификат.

6.6.2. Известить Удостоверяющий центр об изменениях в документах, приведенных в п.4.2. и предоставить актуальные документы в течение 5-ти рабочих дней с момента регистрации изменений, при необходимости провести перерегистрацию Пользователя УЦ и внеплановую смену сертификата.

6.6.3. Пользователь Удостоверяющего центра обязан:

6.6.3.1. Обеспечивать конфиденциальность ключей электронных подписей, в частности, не допускать использование принадлежащего ему ключа электронной подписей без согласия.

6.6.3.2. Применять для формирования электронной подписи только ключ электронной подписи, срок действия сертификата ключа проверки электронной подписи которого не истек.

6.6.3.3. Не применять ключ электронной подписи, если стало известно, что этот ключ используется или использовался ранее другими лицами.

6.6.3.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате.

6.6.3.5. Не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр для приостановления действия или аннулирования сертификата, при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена, а также в случае если стало известно, что этот ключ используется или использовался ранее другими лицами.

6.6.3.6. Не использовать ключ электронной подписи, соответствующий сертификату, заявление на отзыв которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на отзыв сертификата в Удостоверяющий центр по момент времени официального уведомления об отзыве сертификата, либо об отказе в его отзыве.

6.6.3.7. Не использовать ключ электронной подписи, соответствующий сертификату, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

6.6.3.8. Не использовать ключ проверки электронной подписи, соответствующий сертификату, который отозван или действие которого приостановлено.

6.6.3.9. Не использовать ключ проверки электронной подписи до предоставления Удостоверяющему центру подписанной копии сертификата, соответствующего данному ключу проверки электронной подписи.

6.6.3.10. При получении сертификата ознакомиться с информацией, включаемой в сертификат.

6.6.3.11. В случае самостоятельного создания ключа электронной подписи предоставить в Удостоверяющий центр запрос на сертификат в электронном виде, сформированный с использованием средств электронной подписи, совместимых с используемыми средствами Удостоверяющего центра, а также надлежащим образом оформленное заявление на изготовление сертификата. Запрос на сертификат должен содержать всю информацию, предоставляемую для включения в сертификат, в том числе информацию об используемых средствах электронной подписи.

7. Ответственность сторон.

7.1. Удостоверяющий центр несет ответственность за вред, причиненный третьим лицам в результате неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения в области использования электронных подписей, а также настоящим Регламентом.

7.2. Удостоверяющий центр не несет ответственности в случае нарушения Клиентом или Пользователем УЦ положений настоящего Регламента.

7.3. Удостоверяющий центр не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях и других документах Клиента или Пользователя УЦ.

7.4. Стороны не несут ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

7.5. Ответственность сторон, не урегулированная положениями настоящего Регламента, регулируется Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения в области использования электронных подписей.

8. Разрешение споров.

8.1. Сторонами в споре, в случае его возникновения, считаются Министерство и Сторона, присоединившаяся к Регламенту.

8.2. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны руководствуются нормативными правовыми актами Российской Федерации и нормативными правовыми актами Чувашской Республики.

8.3. Стороны будут принимать все необходимые меры к тому, 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. К ответу должны быть приложены все необходимые документы.

8.5. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде Чувашской Республики.

9. Порядок предоставления и пользования услугами Удостоверяющего центра.

9.1. Регистрация пользователя в Удостоверяющем центре и изготовление первого сертификата ключа проверки электронной подписи.

Удостоверяющий центр осуществляет регистрацию Пользователя УЦ только в том случае, если Заявитель присоединился к Регламенту, в соответствии с пунктом 3.4 настоящего Регламента.

9.1.1. Регистрация пользователя в Удостоверяющем центре.

9.1.1.1. Регистрация Пользователя УЦ осуществляется на основании заявления на регистрацию Пользователя УЦ и документов, предоставляемых в соответствии с пунктом 4.2 настоящего Регламента, при личном прибытии в Удостоверяющий центр Уполномоченного представителя Заявителя. Дата и время прибытия в Удостоверяющий центр предварительно согласовывается с Оператором УЦ.

9.1.1.2. Формы заявлений на регистрацию Пользователя УЦ приведены в Приложении № 3 (для Уполномоченного представителя юридического лица) и Приложении № 8 (для юридического лица) настоящего Регламента. Оформленное заявление должно содержать все необходимые реквизиты (дата, исходящий номер, собственноручные подписи и печать организации). Рекомендации по заполнению полей табличной формы заявления на регистрацию Пользователя УЦ для включения информации в сертификат, формируемый при регистрации Пользователя УЦ, приведены в Приложении № 20 настоящего Регламента.

9.1.1.3. Предоставление заявительных документов может быть осуществлено Доверенным лицом Клиента, действующим на основании соответствующей доверенности, которая должна быть составлена по форме, установленной в Приложении № 4 или Приложении № 9 настоящего Регламента.

9.1.1.4. Совместно с заявлением на регистрацию Пользователя УЦ Оператору УЦ предоставляются надлежащим образом заверенные копии документов для подтверждения информации, указанной в заявлении, а именно:

- для подтверждения адреса и наименования организации, в т.ч. сокращенного наименования: копию устава или положения организации (первые страницы, включая страницу, содержащую наименование и адрес организации) или актуальную копию выписки из единого государственного реестра юридических лиц;
- для подтверждения ОГРН: копию свидетельства о государственной регистрации юридического лица;
- для подтверждения ИНН: копию свидетельства о постановке на учет в налоговом органе;
- для подтверждения ФИО: копию основного документа, удостоверяющего личность (копию 2-3 стр. паспорта);
- для подтверждения СНИЛС: копию страхового свидетельства государственного пенсионного страхования физического лица;
- для подтверждения полномочий физического лица действовать от имени юридического лица в соответствии с учредительными документами: копию приказа (распоряжения, протокола) или иного документа о назначении уполномоченным лицом (руководителем) организации.

9.1.1.5. Если какие-либо из вышеприведенных документов предоставлялись Клиентом ранее и не утратили актуальности, повторного предоставления таких документов не требуется.

9.1.1.6. Оператор УЦ осуществляет процедуру идентификации регистрируемого лица или Доверенного лица Клиента путем установления личности по паспорту, выполняет проверку предоставленных заявительных документов и достоверности сведений, указанных в заявительных документах, выполняет действия по регистрации Пользователя УЦ и занесению информации в реестр Удостоверяющего центра.

9.1.1.7. В случае непредставления необходимых документов, ненадлежащего их оформления, предоставления документов не в полном объеме или предоставления документов, подлинность которых вызывает сомнение, Оператор УЦ не осуществляет регистрацию Пользователя УЦ и возвращает документы непосредственно регистрируемому лицу или Доверенному лицу Клиента с объяснением причин.

9.1.2. Изготовление первого сертификата ключа проверки электронной подписи в процессе регистрации Пользователя УЦ.

9.1.2.1. После регистрации Пользователя УЦ Оператор УЦ осуществляет формирование и запись ключа электронной подписи Пользователя УЦ на предоставленный Пользователем УЦ ключевой носитель, изготовление и запись сертификата ключа проверки электронной подписи и печать копии сертификата ключа проверки электронной подписи на бумажном носителе в двух экземплярах по форме, установленной в настоящем Регламенте.

9.1.2.2. Два экземпляра копии сертификата Пользователя УЦ на бумажном носителе визируются личной подписью Оператора УЦ, заверяются печатью и предоставляются непосредственно Пользователю УЦ.

9.1.2.3. Пользователь УЦ или Доверенное лицо Клиента осуществляет проверку включенной в сертификат информации, подписывает собственноручной подписью два экземпляра копии сертификата ключа проверки электронной подписи, один из которых возвращает Оператору УЦ.

По окончании процедуры изготовления первого сертификата ключа проверки электронной подписи непосредственно Пользователю УЦ или Доверенному лицу Клиента выдаются:

- ключевой носитель, содержащий ключ электронной подписи и ключ проверки электронной подписи;
- сертификат ключа проверки электронной подписи Пользователя УЦ в электронной форме, соответствующий ключу электронной подписи;
- сертификат ключа проверки электронной подписи Пользователя УЦ на бумажном носителе;
- сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра в электронной форме;
- руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи в электронной форме;
- лицензия на право использования средств электронной подписи, если необходимость её предоставления указана в заявлении на регистрацию.

9.1.2.4. В процессе регистрации Пользователь УЦ либо доверенное лицо Клиента сообщает Оператору УЦ ключевую фразу, используемую для аутентификации Пользователя УЦ при выполнении регламентных процедур, возникающих при компрометации ключа электронной подписи Пользователя УЦ.

9.1.2.5. Факт передачи фиксируется в журнале поэкземплярного учета СКЗИ Удостоверяющего центра, учёт СКЗИ пользователями производится самостоятельно в соответствии с Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152.

9.2. Изготовление сертификата ключа проверки электронной подписи Пользователя УЦ при плановой и внеплановой смене ключей электронной подписи.

9.2.1. Изготовление ключа электронной подписи и сертификата Пользователя УЦ при плановой смене ключей осуществляется на основании заявления на изготовление сертификата ключа проверки электронной подписи.

9.2.2. Формы заявлений на изготовление сертификата ключа проверки электронной подписи Пользователя УЦ приведены в Приложении № 5 (для Уполномоченного представителя юридического лица) и Приложении № 10 (для юридического лица) настоящего Регламента. Оформленное заявление должно содержать все необходимые реквизиты (дата, исходящий номер).

9.2.3. Заявление на изготовление сертификата ключа проверки электронной подписи оформляется Пользователем УЦ в соответствии с идентификационными данными, указанными ранее при регистрации Пользователя УЦ (данными, содержащимися в поле «Владелец сертификата» бланка сертификата Пользователя УЦ и данными поля Subject сертификата в электронной форме). В случае изменения регистрационных данных производится перерегистрация Пользователя УЦ в соответствии с пунктом 9.1 настоящего Регламента и, при необходимости, отзыв (аннулирование) ранее выданного сертификата.

9.2.4. Заявление на изготовление сертификата может подаваться в Удостоверяющий центр в бумажной форме при личном прибытии Пользователя УЦ или Доверенного лица Клиента в Удостоверяющий центр, либо в электронной форме с рабочего места Пользователя УЦ с использованием АРМ Пользователя Удостоверяющего центра.

9.2.5. Изготовление сертификата Пользователя УЦ по заявлению, поданному в бумажной форме.

9.2.5.1. Заявление на изготовление сертификата ключа проверки электронной подписи подается в Удостоверяющий центр в бумажной форме при личном прибытии Пользователя УЦ в Удостоверяющий центр. Дата и время прибытия в Удостоверяющий центр предварительно согласовывается с Оператором УЦ.

9.2.5.2. Предоставление заявительных документов может быть осуществлено Доверенным лицом Клиента, действующим на основании соответствующей доверенности, которая должна быть составлена по форме, установленной в Приложении № 6 или Приложении № 11 настоящего Регламента.

9.2.5.3. Оператор УЦ осуществляет процедуру идентификации Пользователя УЦ или Доверенного лица Клиента, выполняет проверку предоставленных заявительных документов, и при положительной проверке предоставленных заявительных документов осуществляет формирование и запись ключа электронной подписи на предоставленный Пользователем УЦ ключевой носитель, изготовление и запись сертификата ключа проверки электронной подписи и распечатывает копии сертификата ключа проверки электронной подписи на бумажном носителе в двух экземплярах по форме, установленной в настоящем Регламенте.

9.2.5.4. Два экземпляра копии сертификата Пользователя УЦ на бумажном носителе визируются Оператором УЦ, заверяются печатью и предоставляются непосредственно Пользователю УЦ или Доверенному лицу Клиента.

9.2.5.5. Пользователь УЦ или Доверенное лицо Клиента осуществляет проверку включенной в сертификат информации, подписывает собственноручной подписью два экземпляра копии сертификата ключа проверки электронной подписи, один из которых возвращает непосредственно Оператору УЦ.

По окончании процедуры плановой смены сертификата ключа проверки электронной подписи непосредственно Пользователю УЦ или Доверенному лицу Клиента выдаются:

- ключевой носитель, содержащий ключ электронной подписи;

- сертификат ключа проверки электронной подписи Пользователя УЦ в электронной форме, соответствующий ключу электронной подписи;
- сертификат ключа проверки электронной подписи Пользователя УЦ на бумажном носителе;
- сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра в электронной форме;

9.2.6. Изготовление сертификата Пользователя УЦ по заявлению, поданному в электронной форме.

9.2.6.1. Изготовление сертификата ключа проверки электронной подписи при плановой смене ключей осуществляется на основании заявления на изготовление сертификата Пользователя УЦ и запроса на сертификат ключа проверки электронной подписи, которые предоставляются в Удостоверяющий центр в электронной форме.

9.2.6.2. Заявление на изготовление сертификата ключа проверки электронной подписи, предоставляемое в Удостоверяющий центр в электронной форме, подписывается действующими ключами электронной подписи Пользователя УЦ и уполномоченного представителя юридического лица с использованием средств электронной подписи (например, приложения КриптоАРМ), предоставляемых Удостоверяющим центром, либо приобретаемых Клиентом самостоятельно.

9.2.6.3. Запрос на сертификат ключа проверки электронной подписи представляет собой электронный документ формата CMS. В качестве подписываемых данных используется запрос на сертификат в формате PKCS#10, а электронная подпись запроса осуществляется с использованием действующего ключа электронной подписи Пользователя УЦ.

9.2.6.4. Формирование запроса на изготовление сертификата может быть осуществлено с использованием web-интерфейса АРМ Пользователя УЦ, согласно документации «КриптоПро УЦ. Руководство пользователя», либо с использованием стороннего программного обеспечения, совместимого со средствами Удостоверяющего центра (приложение командной строки cryptsp, приложение КриптоАРМ).

9.2.6.5. Значение поля Subject, содержащееся в запросе на сертификат, должно быть идентично идентификационным данным, указанным в заявлении на изготовление сертификата, а также идентично значению этого поля в сертификате, соответствующему действующему ключу электронной подписи Пользователя УЦ, с использованием которого подписано заявление на изготовление сертификата Пользователя УЦ и запрос на сертификат.

9.2.6.6. Способ предоставления запроса на сертификат (если запрос сформирован без использования web-интерфейса АРМ Пользователя УЦ) и заявления на изготовление сертификата в электронной форме определяется Пользователем УЦ по согласованию с Удостоверяющим центром.

9.2.6.7. После получения заявления и запроса на изготовление сертификата Оператор УЦ осуществляет проверку электронной подписи заявления и запроса на изготовление сертификата Пользователя УЦ, а также идентификационных данных, указанных в заявлении и запросе на изготовление сертификата.

9.2.6.8. В случае отрицательного результата проведенных проверок заявительных документов, ненадлежащего оформления заявительных документов, а также иных случаях, установленных настоящим Регламентом, Оператор УЦ отклоняет заявление и запрос на сертификат и не позднее 1 (одного) рабочего дня с момента отклонения запроса уведомляет Пользователя УЦ о причинах отказа в изготовлении сертификата.

9.2.6.9. При положительном результате проверок заявительных документов, Оператор УЦ осуществляет изготовление и предоставление Пользователю УЦ сертификата ключа проверки электронной подписи. Если запрос на сертификат был предоставлен без использования web-интерфейса АРМ Пользователя УЦ, способ

предоставления сертификата определяется Удостоверяющим центром по согласованию с Пользователем УЦ.

9.2.6.10. Изготовление сертификата ключа проверки электронной подписи и уведомление Пользователя УЦ об изготовлении сертификата осуществляются не позднее 3 (трех) рабочих дней следующих за рабочим днем, в течение которого было получено заявление на изготовление сертификата.

9.2.6.11. После получения уведомления об изготовлении сертификата Пользователь УЦ с помощью АРМ пользователя УЦ производит установку сертификата на своем рабочем месте и подтверждает ее.

9.2.6.12. После изготовления сертификата ключа проверки электронной подписи Оператор УЦ формирует и подписывает копию сертификата и направляет Пользователю УЦ.

9.2.6.13. До истечения 10 (десяти) календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и предоставить в Удостоверяющий центр копию сертификата ключа проверки электронной подписи.

9.2.7. Изготовление сертификата ключа проверки электронной подписи Пользователя УЦ при внеплановой смене ключей электронной подписи.

9.2.7.1. Внеплановая смена ключей осуществляется Пользователем УЦ в следующих случаях:

- При компрометации ключа электронной подписи Пользователя УЦ;
- При компрометации ключа электронной подписи уполномоченного лица УЦ;
- В случае, если Пользователь УЦ по каким-либо причинам не смог осуществить плановую смену ключей электронной подписи в установленные для этой процедуры сроки;
- В иных случаях, вызванных форс-мажорными обстоятельствами

9.2.7.2. Изготовление сертификата Пользователя УЦ производится на основании заявления на изготовление сертификата ключа проверки электронной подписи, предоставляемого в бумажной или электронной форме, в соответствии с пунктами 9.2.1-9.2.6 настоящего Регламента.

9.2.7.3. В случае, если срок действия ключа электронной подписи Пользователя УЦ истек, а также в иных случаях невозможности использования ключа электронной подписи (компрометация, выход из строя ключевого носителя и т.п.), изготовление сертификата Пользователя УЦ производится по заявлению на изготовление сертификата, предоставляемого в бумажной форме, в соответствии с пунктами 9.2.1 - 9.2.5 настоящего Регламента.

9.2.7.4. В случае компрометации ключа электронной подписи Пользователя УЦ производится приостановление действия ключа проверки электронной подписи в соответствии с пунктом 9.4.9 Регламента.

9.3. Аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра.

9.3.1. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи Пользователя УЦ в следующих случаях:

- по истечении срока его действия;
- в случае прекращения действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту;
- по истечении срока, на который действие сертификата ключа проверки электронной подписи было приостановлено;
- по заявлению Клиента или Пользователя УЦ;
- при компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра;

- в случае прекращения деятельности Удостоверяющего центра без передачи его функций другим лицам;
- в иных случаях, предусмотренных нормативными правовыми актами Российской Федерации.

9.3.2. В случае прекращения действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту, истечения срока, на который действие сертификата ключа проверки электронной подписи было приостановлено, отзыва сертификата по заявлению Клиента или Пользователя УЦ, Удостоверяющий центр обязан не позднее 7 (семи) календарных дней со дня аннулирования сертификата официально уведомить Пользователя УЦ и всех лиц, зарегистрированных в Удостоверяющем центре, об аннулировании сертификата.

9.3.3. Официальным уведомлением о факте отзыва сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем отзыва сертификата признается время издания указанного списка отозванных сертификатов, хранящееся в поле «Действителен с» списка отозванных сертификатов.

9.3.4. Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей подписей в расширение «Точка распространения списка отозванных сертификатов» сертификата ключа проверки электронной подписи Пользователя УЦ.

9.3.5. В случае отзыва сертификата ключа проверки электронной подписи Пользователя УЦ по истечении срока его действия датой и временем отзыва сертификата ключа проверки электронной подписи Пользователя УЦ признаются дата и время, хранящиеся в поле «Действителен по» сертификата ключа проверки электронной подписи. В данном случае информация об отозванном сертификате ключа проверки электронной подписи Пользователя УЦ в список отозванных сертификатов не заносится.

9.3.6. В случае компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра временем отзыва сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра признаются дата и время компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра, фиксирующееся в реестре Удостоверяющего центра. В случае компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра информация о сертификате ключа проверки электронной подписи пользователя Удостоверяющего центра в список отозванных сертификатов не заносится.

9.3.7. Аннулирование сертификата ключа проверки электронной подписи осуществляется по заявлению Клиента, подающемуся в Удостоверяющий центр в электронной или бумажной форме. Формы заявлений на аннулирование (отзыв) сертификата ключа проверки электронной подписи приведены в Приложении № 7 (для Уполномоченного представителя юридического лица) и Приложении № 12 (для юридического лица) настоящего Регламента. Оформленное заявление должно содержать все необходимые реквизиты (дата, исходящий номер).

9.3.8. Аннулирование сертификата ключа проверки электронной подписи Пользователя УЦ на основании заявления в бумажной форме.

9.3.8.1. Заявление на аннулирование сертификата в бумажной форме предоставляется в Удостоверяющий центр при личном прибытии Пользователя УЦ в Удостоверяющий центр, либо посредством почтовой или курьерской связи.

9.3.8.2. После получения заявления на аннулирование сертификата Оператор УЦ принимает решение об аннулировании сертификата Пользователя УЦ.

9.3.8.3. В случае ненадлежащего оформления заявительных документов Оператор УЦ не осуществляет аннулирование сертификата и не позднее 1 (одного) рабочего дня со

дня поступления заявительных документов уведомляет об этом Пользователя УЦ с указанием причин отклонения заявления.

9.3.8.4. При положительной проверке заявительных документов Оператор УЦ осуществляет аннулирование сертификата ключа проверки электронной подписи Пользователя УЦ.

9.3.8.5. Аннулирование сертификата ключа проверки электронной подписи и официальное уведомление Пользователя УЦ об аннулировании сертификата должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было предоставлено заявление.

9.3.9. Аннулирование сертификата ключа проверки электронной подписи Пользователя УЦ на основании заявления в электронной форме.

9.3.9.1. Аннулирование сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется на основании заявления на аннулирование (отзыв) сертификата, предоставляемого в Удостоверяющий центр в электронной форме и запроса на отзыв сертификата, сформированного с использованием web-интерфейса АРМ Пользователя УЦ.

9.3.9.2. Заявление на аннулирование (отзыв) сертификата, предоставляемое в Удостоверяющий центр в электронной форме, подписывается действующими ключами электронной подписи Пользователя УЦ и (или) ключами электронной подписи уполномоченного представителя юридического лица (руководителя организации) с использованием средств электронной подписи (например, приложения КриптоАРМ), предоставляемых Удостоверяющим центром, либо приобретаемых Клиентом самостоятельно.

9.3.9.3. Запрос на отзыв сертификата ключа представляет собой электронный документ формата CMS, подписанный электронной подписью с использованием действующего ключа электронной подписи Пользователя УЦ и направленный в Удостоверяющий центр с использованием web-интерфейса АРМ Пользователя УЦ.

9.3.9.4. После получения заявления на аннулирование сертификата и запроса на отзыв Оператор УЦ осуществляет проверку заявительных документов.

9.3.9.5. В случае ненадлежащего оформления заявительных документов Оператор УЦ не осуществляет аннулирование сертификата и не позднее 1 (одного) рабочего дня со дня поступления заявительных документов уведомляет об этом Пользователя УЦ с указанием причин отклонения заявления.

9.3.9.6. При положительной проверке заявительных документов Оператор УЦ осуществляет аннулирование сертификата ключа проверки электронной подписи Пользователя УЦ.

9.3.9.7. Аннулирование сертификата Пользователя УЦ и официальное уведомление Пользователя УЦ об аннулировании сертификата должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было предоставлено заявление.

9.4. Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ.

9.4.1. Удостоверяющий центр приостанавливает действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в следующих случаях:

- по заявлению Клиента или Пользователя УЦ, предоставляемого в бумажной или электронной форме;
- по заявлению Пользователя УЦ в устной форме в случае компрометации или подозрения в компрометации ключа электронной подписи Пользователя УЦ;
- в иных случаях, предусмотренных положениями настоящего Регламента, по решению Удостоверяющего центра.

9.4.2. Действие сертификата ключа проверки электронной подписи приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата ключа подписи составляет 10 (десять) дней.

9.4.3. Если в течение срока приостановления действия сертификата ключа проверки электронной подписи действие этого сертификата не будет возобновлено, то данный сертификат отзывается Удостоверяющим центром.

9.4.4. Официальным уведомлением о факте приостановления действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, и изданного не ранее времени наступления произошедшего случая. Датой и временем приостановления действия сертификата ключа проверки электронной подписи признаются дата и время издания указанного списка отозванных сертификатов, хранящееся в поле «Действителен с» списка отозванных сертификатов.

9.4.5. Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей проверки электронных подписей в расширение «Точка распространения списка отзыва» сертификата ключа проверки электронной подписи.

9.4.6. Приостановление действия сертификата ключа проверки электронной подписи осуществляется по заявлению Клиента или Пользователя УЦ, которое предоставляется в Удостоверяющий центр в бумажной, электронной или устной форме, а также по решению Удостоверяющего центра в случаях, определенных настоящим Регламентом. Формы заявлений на приостановление действия сертификата ключа проверки электронной подписи приведены в Приложении № 13 (для Уполномоченного представителя юридического лица) и Приложении № 14 (для юридического лица) настоящего Регламента. Оформленное заявление должно содержать все необходимые реквизиты (дата, исходящий номер).

9.4.7. Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ на основании заявления в бумажной форме.

9.4.7.1. Заявление в бумажной форме предоставляется в Удостоверяющий центр при личном прибытии Пользователя УЦ в Удостоверяющий центр, либо предоставляемого посредством почтовой или курьерской связи.

9.4.7.2. После проверки заявительных документов Оператор УЦ принимает решение о приостановлении действия сертификата ключа проверки электронной подписи.

9.4.7.3. В случае ненадлежащего оформления заявительных документов Оператор УЦ отклоняет заявление о приостановлении действия сертификата и уведомляет об этом Пользователя УЦ в течение 1 (одного) рабочего дня с обоснованием причин.

9.4.7.4. При положительной проверке заявительных документов Оператор УЦ в течение 1 (одного) рабочего дня приостанавливает действие сертификата ключа проверки электронной подписи.

9.4.8. Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ на основании заявления в электронной форме.

9.4.8.1. Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется на основании заявления на приостановление действия сертификата, предоставляемого в Удостоверяющий центр в электронной форме и запроса на приостановление действия сертификата, сформированного с использованием web-интерфейса АРМ Пользователя УЦ.

9.4.8.2. Заявление на приостановление действия сертификата, предоставляемое в Удостоверяющий центр в электронной форме, подписывается действующими ключами электронной подписи Пользователя УЦ и (или) ключами электронной подписи

уполномоченного представителя юридического лица (руководителя организации) с использованием средств электронной подписи (например, приложения КриптоАРМ), предоставляемых Удостоверяющим центром, либо приобретаемых Клиентом самостоятельно.

9.4.8.3. Запрос на приостановление действия сертификата ключа представляет собой электронный документ формата CMS, подписанный электронной подписью с использованием действующего ключа электронной подписи Пользователя УЦ и направленный в Удостоверяющий центр с использованием web-интерфейса АРМ Пользователя УЦ.

9.4.8.4. После получения заявления на приостановление действия сертификата и запроса на отзыв Оператор УЦ принимает решение о приостановлении действия сертификата Пользователя УЦ.

9.4.8.5. В случае ненадлежащего оформления заявительных документов Оператор УЦ отклоняет заявление о приостановлении действия сертификата и уведомляет об этом Пользователя УЦ в течение 1 (одного) рабочего дня с обоснованием причин.

9.4.8.6. При положительной проверке заявительных документов Оператор УЦ в течение 1 (одного) рабочего дня приостанавливает действие сертификата ключа проверки электронной подписи Пользователя УЦ.

9.4.9. Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ на основании заявления в устной форме.

9.4.9.1. Приостановление действия сертификата ключа проверки электронной подписи по заявлению Пользователя УЦ в устной форме осуществляется исключительно при компрометации ключа электронной подписи или подозрении в компрометации ключа электронной подписи пользователя Удостоверяющего центра.

9.4.9.2. Заявление подается Оператору УЦ по телефону.

9.4.9.3. Пользователь УЦ должен сообщить Оператору УЦ следующую информацию:

- идентификационные данные, содержащиеся в сертификате ключа проверки электронной подписи, действие которого необходимо приостановить;
- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключа проверки электронной подписи;
- ключевую фразу Пользователя УЦ (ключевая фраза определяется в процессе регистрации и изготовления первого сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра).

9.4.9.4. Заявление Оператором принимается только в случае положительной аутентификации Пользователя УЦ (совпадения ключевой фразы, сообщаемой при регистрации Пользователя УЦ, с информацией из реестра зарегистрированных пользователей Удостоверяющего центра).

9.4.9.5. После получения в устной форме заявления на приостановление действия сертификата ключа проверки электронной подписи Оператор в течение 1 (одного) рабочего дня приостанавливает действие сертификата Пользователя УЦ.

9.4.9.6. Не позднее 5 (пяти) рабочих дней с момента приостановления действия сертификата ключа проверки электронной подписи Пользователь УЦ должен направить в Удостоверяющий центр заявление на аннулирование сертификата ключа проверки электронной подписи в бумажной форме в том случае, если факт компрометации ключа электронной подписи подтвердился, либо заявление на возобновление действия сертификата ключа проверки электронной подписи в случае, если факт компрометации ключа электронной подписи не подтвердился.

9.4.10. Приостановление действия сертификата ключа проверки электронной подписи по решению Удостоверяющего центра.

9.4.10.1. Удостоверяющий центр вправе приостановить действие сертификата ключа проверки электронной подписи Пользователя УЦ в случаях компрометации или подозрения в компрометации ключа электронной подписи пользователя УЦ в том случае, если Пользователю УЦ не было известно о возможном факте компрометации ключей.

9.4.10.2. После приостановления действия сертификата ключа проверки электронной подписи Оператор УЦ сообщает Пользователю УЦ о наступлении события, повлекшего приостановление действия сертификата, и в течение 1 (одного) рабочего дня уведомляет его о том, что действие сертификата Пользователя УЦ приостановлено.

9.5. Возобновление действия сертификата ключа проверки электронной подписи Пользователя УЦ.

9.5.1. Заявление возобновление действия сертификата предоставляется в бумажной форме по форме Приложения № 15 (для Уполномоченного представителя юридического лица) или Приложения № 16 (для юридического лица) при личном прибытии Пользователя УЦ в Удостоверяющий центр, либо посредством почтовой или курьерской связи.

9.5.2. После предоставления заявления ответственное лицо Удостоверяющего центра принимает решение о возобновлении действия сертификата ключа подписи.

9.5.3. В случае ненадлежащего оформления заявительных документов Оператор УЦ не возобновляет действие сертификата уведомляет об этом Пользователя УЦ в течение 1 (одного) дня с указанием причины отклонения заявления.

9.5.4. При положительной проверке заявительных документов Оператор УЦ в течение 1 (одного) рабочего дня возобновляет действие сертификата ключа проверки электронной подписи Пользователя УЦ.

9.5.5. Официальным уведомлением о факте возобновления действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, не содержащего сведения о сертификате, действие которого было возобновлено, и изданного не ранее времени предоставления заявления на возобновление действия сертификата. Временем возобновления действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле «Действителен с» списка отозванных сертификатов.

9.5.6. Возобновление действия сертификата ключа проверки электронной подписи возможно только в течение срока, на который действие сертификата ключа подписи было приостановлено.

9.6. Получение информации о статусе сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром.

9.6.1. Получение информации о статусе сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром, осуществляется на основании заявления о получении соответствующей информации. Данное заявление оформляется по форме Приложения № 17 к настоящему Регламенту и предоставляется в Удостоверяющий центр в бумажной форме при личном прибытии Пользователя УЦ. Заявление может быть направлено в Удостоверяющий центр с использованием почтовой или курьерской связи, либо предоставлено в форме электронного документа, подписанного с использованием ключа электронной подписи Пользователя УЦ.

9.6.2. Заявление должно содержать следующую информацию:

- время и дата подачи заявления;
- время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключа проверки электронной подписи;

- идентификационные данные пользователя Удостоверяющего центра, статус сертификата ключа проверки электронной подписи которого требуется установить;
- серийный номер сертификата ключа проверки электронной подписи, статус которого требуется установить.

9.6.3. По результатам проведения работ Оператором УЦ оформляется справка, содержащая информацию о статусе сертификата ключа проверки электронной подписи, которая предоставляется заявителю.

9.6.4. Предоставление пользователю Удостоверяющего центра справки о статусе сертификата ключа проверки электронной подписи осуществляется в течение 5 (пяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

9.7. Подтверждение подлинности электронной подписи в электронном документе.

9.7.1. Подтверждение подлинности электронной подписи в электронном документе осуществляется на основании заявления, направляемого Пользователем УЦ по форме Приложения № 18 настоящего Регламента.

9.7.2. Заявление должно содержать следующую информацию:

- дату и регистрационный номер заявления;
- идентификационные данные пользователя, подлинность электронной подписи которого необходимо подтвердить в электронном документе;
- время и дату формирования электронной подписи электронного документа;
- время и дату, на момент наступления которых требуется установить подлинность электронной подписи.

9.7.3. Обязательным приложением к заявлению на подтверждение подлинности электронной подписи в электронном документе является носитель информации, содержащий:

- сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе - в виде файла стандарта криптографических сообщений Cryptographic Message Syntax (CMS);
- электронный документ в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

9.7.4. Проведение работ по подтверждению подлинности электронной подписи в электронном документе осуществляет комиссия, сформированная из числа сотрудников Министерства.

9.7.5. По результатам проведения работ по подтверждению подлинности электронной подписи в электронном документе оформляется заключение.

9.7.6. Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки электронной подписи электронного документа;
- данные, представленные комиссии для проведения проверки;
- отчет по выполненной проверке.

9.7.7. Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки.

9.7.8. Заключение по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

9.7.9. Срок проведения работ по подтверждению подлинности электронной подписи в одном электронном документе и предоставлению заявителю заключения по выполненной проверке составляет не более 10 (десяти) рабочих дней с момента поступления соответствующего заявления.

9.8. Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени.

9.8.1. Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе сертификатов посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам пользователей Удостоверяющего центра формирует и предоставляет этим пользователям OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного с использованием ключа электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов).

OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- подтверждена подлинность электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) в OCSP-ответе;
- сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент подтверждения подлинности электронной подписи OCSP-ответа действителен;
- ключ электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;
- сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении Extended Key Usage область использования – Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9).

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра – <http://ocsp.cap.ru/ocsp/ocsp.srf>

Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых Удостоверяющим центром сертификатов ключей проверки электронной подписи.

9.8.2. Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени.

Штамп времени, относящийся к подписанному электронной подписью электронному документу, признается действительным при одновременном выполнении следующих условий:

- подтверждена подлинность электронной подписи Службы штампов времени (Оператора Службы штампов времени) в штампе времени;
- сертификат ключа проверки электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности ЭЦП штампа времени действителен;
- ключ электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;
- сертификат ключа проверки электронной подписи Службы штампов времени (Оператора Службы штампов времени) содержит в расширении Extended Key Usage область использования – Установка штампа времени (1.3.6.1.5.5.7.3.8);

Адрес обращения к Службе штампов времени Удостоверяющего центра – <http://tsp.cap.ru/tsp/tsp.srf>

10. Смена ключей уполномоченного лица Удостоверяющего центра.

10.1. Плановая смена ключей уполномоченного лица Удостоверяющего центра.

10.1.1. Плановая смена ключа электронной подписи и соответствующего ему сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра выполняется в период действия ключа электронной подписи уполномоченного лица Удостоверяющего центра.

10.1.2. Процедура плановой смены ключей уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:

- уполномоченное лицо Удостоверяющего центра формирует новый ключ электронной подписи и соответствующий ему ключ проверки подписи;
- уполномоченное лицо Удостоверяющего центра изготавливает сертификат ключа проверки электронной подписи и подписывает его созданным ключом электронной подписи.

10.1.3. Уведомление пользователей о проведении плановой смены ключей уполномоченного лица Удостоверяющего центра осуществляется в течение 1 (одного) рабочего дня посредством публикации соответствующей информации на сайте Удостоверяющего центра по адресу <http://www.cap.ru/certsrv>

10.1.4. Предыдущий (подвергшийся процедуре плановой смены) ключ электронной подписи уполномоченного лица Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия предыдущего ключа электронной подписи уполномоченного лица Удостоверяющего центра.

10.2. Внеплановая смена ключей уполномоченного лица Удостоверяющего центра.

10.2.1. Внеплановая смена ключей уполномоченного лица Удостоверяющего центра выполняется в случае компрометации или угрозы компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра.

10.2.2. В случае компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра сертификат уполномоченного лица Удостоверяющего центра аннулируется (отзывается). Все сертификаты, подписанные с использованием скомпрометированного ключа электронной подписи уполномоченного лица Удостоверяющего центра, считаются аннулированными.

10.2.3. Уведомление Пользователей УЦ о компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра осуществляется в течение 1 (одного) рабочего дня посредством публикации соответствующей информации на сайте Удостоверяющего центра <http://www.cap.ru/certsrv> и рассылки Пользователям УЦ уведомления по электронной почте.

10.2.4. После аннулирования сертификата уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица Удостоверяющего центра, в соответствии с пунктом 10.1 настоящего Регламента.

10.2.5. Все подписанные с использованием скомпрометированного ключа электронной подписи уполномоченного лица Удостоверяющего центра и действовавшие на момент компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра сертификаты ключей проверки электронной подписи, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене в соответствии с пунктом 9.2.7 настоящего Регламента.

11. Конфиденциальность информации.

11.1. Типы конфиденциальной информации

11.1.1. Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не осуществляет хранение ключей электронных подписей пользователей Удостоверяющего центра.

11.1.2. Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, содержащаяся в Реестре Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.

11.2. Типы информации, не являющейся конфиденциальной.

11.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

11.2.2. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.

11.2.3. Информация, включаемая в сертификаты ключей проверки электронной подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

11.2.4. Персональные данные, включаемые в сертификаты ключей проверки электронных подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

11.2.5. Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

11.3. Исключительные полномочия Удостоверяющего центра.

Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных нормативными правовыми актами Российской Федерации и нормативными правовыми актами Чувашской Республики.

11.4. Обработка персональных данных пользователей удостоверяющего центра.

11.4.1. Целью обработки персональных данных является выполнение функций удостоверяющего центра по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иных функций, предусмотренных Федеральным законом «Об электронной подписи».

11.4.2. Обработка персональных данных осуществляется Удостоверяющим центром на основании письменного согласия лица, регистрирующегося в реестре Удостоверяющего центра.

11.4.3. Сторона, присоединившаяся к Регламенту Удостоверяющего центра, соглашается на обработку Удостоверяющим центром персональных данных, включаемых в сертификат ключа проверки электронной подписи, а также персональных данных, необходимых для идентификации и аутентификации субъекта персональных данных в качестве Владельца сертификата, пользователя информационных систем и участника межведомственного электронного взаимодействия органов государственной Чувашской Республики.

11.4.4. Пользователь УЦ соглашается, что персональные данные, включаемые в сертификат ключа проверки электронной подписи, являются общедоступными персональными данными, к которым относятся: Фамилия, Имя, Отчество, номер страхового свидетельства государственного пенсионного страхования, идентификационный номер налогоплательщика. С согласия субъекта персональных данных в сертификат ключа проверки электронной подписи может быть включена иная информация о Владельце сертификата.

11.4.5. Удостоверяющий центр осуществляет следующие действия с персональными данными: сбор, систематизацию, использование, распространение и хранение персональных данных.

11.4.6. Сбор и систематизация персональных данных пользователей УЦ осуществляется в ходе приема заявлений от лиц, проходящих процедуру регистрации в соответствии с настоящим Регламентом.

11.4.7. Полученные персональные данные используются для регистрации пользователей УЦ в реестре Удостоверяющего центра и для изготовления сертификатов ключей проверки электронной подписи.

11.4.8. Удостоверяющий центр обеспечивает защиту персональных данных от уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

11.4.9. Список должностных лиц удостоверяющего центра, допущенных к обработке персональных данных пользователей УЦ, утверждается приказом министра информационной политики и массовых коммуникаций Чувашской Республики.

11.4.10. Согласие на обработку персональных данных Пользователя УЦ может быть отозвано по письменному заявлению Пользователя УЦ, в соответствии с которым производится аннулирование сертификата и прекращение обработки персональных данных Пользователя УЦ, при этом, согласие на обработку персональных данных, содержащихся в сертификатах ключей проверки электронной подписи и реестре сертификатов, не может быть отозвано. В соответствии с Федеральным законом «Об электронной подписи» сертификат ключа проверки электронной подписи и информация, содержащаяся в реестре сертификатов, подлежит хранению в Удостоверяющем центре в течение срока его деятельности.

12. Ведение реестра сертификатов.

12.1. Правила ведения реестра сертификатов и предоставления информации, содержащейся в реестре сертификатов.

12.1.1. Удостоверяющий центр ведет реестр выданных и аннулированных сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования.

12.1.2. Формирование реестра сертификатов осуществляется Удостоверяющим центром в соответствии с Федеральным законом «Об электронной подписи» в порядке, установленном приказом Министерства связи и массовых коммуникаций Российской Федерации от 5 октября 2011 года № 250 «Об утверждении порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».

12.1.3. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов, а также защиту информации от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

12.1.4. Сертификаты ключей проверки электронной подписи и информация, содержащейся в реестре сертификатов, хранится Удостоверяющим центром в электронной форме в течение всего срока деятельности Удостоверяющего центра.

12.1.5. Хранение информации, содержащейся в реестре сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность.

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

12.2. Структура реестра сертификатов.

12.2.1. Реестр сертификатов состоит из следующих разделов:

- сертификаты, выданные юридическим лицам;
- сертификаты, выданные физическим лицам;
- аннулированные сертификаты, выданные юридическим лицам;
- аннулированные сертификаты, выданные физическим лицам;
- сертификаты, выданные юридическим лицам, прекратившие свое действие;
- сертификаты, выданные физическим лицам, прекратившие свое действие.

12.2.2. При выдаче сертификата ключа проверки электронной подписи юридическому лицу Удостоверяющий центр вносит в течение одного рабочего дня в реестр сертификатов следующие сведения:

- уникальный номер сертификата;
- даты начала и окончания действия сертификата;
- наименование, место нахождения и основной государственный регистрационный номер владельца сертификата;
- идентификационный номер налогоплательщика владельца сертификата;
- реквизиты свидетельства о государственной регистрации юридического лица;
- основные реквизиты (наименование, номер и дата выдачи) документа, подтверждающего право лица, выступавшего от имени заявителя, обращаться за получением сертификата;
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца сертификата включена в сертификат;
- ограничения использования сертификата (если такие ограничения устанавливаются);
- иную информацию о владельце сертификата (по требованию заявителя).

12.2.3. При выдаче сертификата ключа проверки электронной подписи физическому лицу Удостоверяющий центр вносит в течение 1 (одного) рабочего дня в реестр сертификатов следующие сведения:

- уникальный номер сертификата;
- даты начала и окончания действия сертификата;
- фамилия, имя и отчество (если имеется) владельца сертификата;
- реквизиты основного документа, удостоверяющего личность владельца сертификата (номер, серия, дата выдачи);
- страховой номер индивидуального лицевого счета владельца сертификата;
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца сертификата включена в сертификат;
- ограничения использования сертификата (если такие ограничения устанавливаются);
- иную информацию о владельце сертификата (по требованию заявителя).

12.2.4. При аннулировании сертификата ключа проверки электронной подписи, владельцем которого является юридическое лицо, Удостоверяющий центр вносит в течение 1 (одного) рабочего дня в реестр сертификатов следующие сведения:

- уникальный номер сертификата;
- даты начала и окончания действия сертификата;
- наименование, место нахождения и основной государственный регистрационный номер владельца сертификата;
- дата аннулирования сертификата;
- основание аннулирования сертификата.

12.2.5. При аннулировании сертификата ключа проверки электронной подписи, владельцем которого является физическое лицо, Удостоверяющий центр вносит в течение 1 (одного) рабочего дня в реестр сертификатов следующие сведения:

- уникальный номер сертификата;
- даты начала и окончания действия сертификата;
- фамилия, имя и отчество (если имеется) владельца сертификата;
- дата аннулирования сертификата;
- основание аннулирования сертификата.

12.2.6. При прекращении действия сертификата ключа проверки электронной подписи, владельцем которого является юридическое лицо, Удостоверяющий центр вносит в течение 1 (одного) рабочего дня в реестр сертификатов следующие сведения:

- уникальный номер сертификата;
- даты начала и окончания действия сертификата;
- наименование, место нахождения и основной государственный регистрационный номер владельца сертификата;
- дата прекращения действия сертификата;
- основание прекращения действия сертификата.

12.2.7. При прекращении действия сертификата ключа проверки электронной подписи, владельцем которого является физическое лицо, Удостоверяющий центр вносит в течение 1 (одного) рабочего дня в реестр сертификатов следующие сведения:

- уникальный номер сертификата;
- даты начала и окончания действия сертификата;
- фамилия, имя и отчество (если имеется) владельца сертификата;
- дата прекращения действия сертификата;
- основание прекращения действия сертификата.

12.3. Предоставление информации, содержащейся в реестре сертификатов.

12.3.1. Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к реестру сертификатов, при этом Удостоверяющий центр не публикует информацию, которая не внесена в сертификаты ключей проверки электронной подписи пользователей УЦ и не относится к категории общедоступных персональных данных.

12.3.2. Информация, содержащаяся в реестре сертификатов, предоставляется Удостоверяющим центром безвозмездно любому лицу по его обращению. Обращение может быть направлено в Удостоверяющий центр в форме бумажного или электронного документа.

12.3.3. Удостоверяющий центр вправе отказать в предоставлении информации, содержащейся в реестре сертификатов, если объем запрашиваемых данных не соответствует законной цели обработки этих данных, заявленной в обращении, а также если обращение содержит запрос персональных данных, не являющихся общедоступными, и согласие субъекта персональных данных на передачу третьим лицам вышеуказанных персональных данных Удостоверяющим центром не получено.

12.3.4. Удостоверяющий центр предоставляет информацию, содержащуюся в реестре сертификатов, в форме выписки из реестра сертификатов.

12.3.5. Срок предоставления информации, содержащейся в реестре сертификатов, направляемой заявителю в форме бумажного документа, составляет не более 7 (семи) рабочих дней со дня поступления обращения.

12.3.6. Срок предоставления информации, содержащейся в реестре сертификатов, направляемой заявителю в форме электронного документа, составляет не более 1 (одного) рабочего дня со дня поступления обращения.

13. Структура сертификатов ключей проверки электронных подписей и сроки действия ключевых документов.

13.1. Структура сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра.

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName (Общее имя) = псевдоним Удостоверяющего центра OrganizationUnit (Подразделение) = Organization (Организация) = LocalityName (Населенный пункт) = Чебоксары State (Область) = 21 Чувашская Республика - Чувашия Country (Страна) = RU Email (Электронная почта) = StreetAddress = Название улицы, номер дома INN (ИНН) = OGRN (ОГРН) =
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName (Общее имя) = псевдоним Удостоверяющего центра OrganizationUnit (Подразделение) = Organization (Организация) = LocalityName (Населенный пункт) = Чебоксары State (Область) = 21 Чувашская Республика - Чувашия Country (Страна) = RU Email (Электронная почта) = StreetAddress = Название улицы, номер дома INN (ИНН) = OGRN (ОГРН) =
Public Key	Открытый ключ	Ключ проверки электронной подписи (алгоритм ГОСТ Р 34.10-2001)
SubjectSignTool	Средство электронной подписи владельца сертификата	Название средства ЭП владельца сертификата
IssuerSignTool	Средства электронной подписи и УЦ издателя	signTool (средство электронной подписи): название средства ЭП signToolCert (заключение на средство ЭП): реквизиты заключения сATool (средство УЦ): название средства УЦ сAToolCert (заключение на средство УЦ): реквизиты заключения
Дополнения сертификата		
Key Usage (critical)	Использование ключа	Цифровая подпись, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (86)
Subject Key Identifier	Идентификатор ключа субъекта	Идентификатор ключа электронной подписи уполномоченного лица Удостоверяющего центра, соответствующего данному сертификату
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата	Версия сертификата уполномоченного лица Удостоверяющего центра
Certificate Policies	Политики сертификата	[1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1 [2]Политика сертификата: Идентификатор политики=Класс средства ЭП КС2
BasicConstraints	Основные ограничения	SubjectType (Тип владельца сертификата) =ЦС Path Length Constraint (Ограничение на длину пути – ограничивает

		количество уровней иерархии при создании подчиненных Удостоверяющих центров) = Отсутствует
--	--	--

13.2. Типовая структура сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра.

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName (Общее имя) = псевдоним Удостоверяющего центра OrganizationUnit (Подразделение) = Organization (Организация) = LocalityName (Населенный пункт) = Чебоксары State (Область) = 21 Чувашская Республика - Чувашия Country (Страна) = RU Email (Электронная почта) = StreetAddress = Название улицы, номер дома INN (ИНН) = OGRN (ОГРН) =
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	Surname = Фамилия GivenName = Имя и Отчество физического лица Title = Должность StreetAddress = Название улицы, номер дома UnstructuredAddress = Неструктурированный адрес = Местонахождение организации CommonName = Наименование организации OrganizationUnit = Подразделение Organization = Наименование организации LocalityName = Наименование населенного пункта State = Субъект Федерации Country = Страна = RU Email = Электронная почта INN = ИНН организации OGRN = ОГРН SNILS = СНИЛС В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 328
Public Key	Открытый ключ	Ключ проверки электронной подписи (алгоритм подписи)
Дополнения сертификата		
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре.
Subject Key Identifier	Идентификатор ключа субъекта	Идентификатор ключа электронной подписи владельца сертификата
Authority Key Identifier	Идентификатор ключа центра сертификатов	Идентификатор ключа электронной подписи уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/name.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, name – имя списка отозванных сертификатов
Authority Information Access	Адрес сертификата центра	URL адреса точки распространения сертификата центра сертификатов

Название	Описание	Содержание
	сертификатов	
SubjectSignTool	Средство электронной подписи владельца сертификата	Название средства ЭП владельца сертификата
PrivateKeyUsagePeriod	Период использования закрытого ключа	Период использования ключа электронной подписи
Certificate Policies	Политики сертификата	Политики сертификата, в т.ч. класс средств ЭП владельца сертификата
IssuerSignTool	Средства электронной подписи и УЦ издателя	signTool (средство электронной подписи): название средства ЭП signToolCert (заключение на средство ЭП): реквизиты заключения сATool (средство УЦ): название средства УЦ сAToolCert (заключение на средство УЦ): реквизиты заключения
Key Usage (critical)	Использование ключа	Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

13.3. Структура списка отозванных сертификатов ключей проверки электронной подписи.

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Атрибуты имени Удостоверяющего центра
Effective date	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
Next update	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
Revoked Certificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (Serial Number) 2. Время аннулирования или время обработки заявления на прекращение действия сертификата (Revocation Date) 3. Код причины отзыва сертификата (CRL Reason Code): "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия
Signature algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего центра, которым подписан СОС
CA Version	Версия сертификата издателя	Версия сертификата Удостоверяющего центра
CRL Number	Номер СОС	Порядковый номер СОС
CRL Next Publish	Следующая публикация СОС	дд.мм.гггг чч:мм:сс GMT

13.4. Расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи содержат объектные идентификаторы (OID), определяющие отношения, при осуществлении которых электронный документ, подписанный ЭП, будет иметь юридическое значение.

13.5. Список типов сертификатов ключей проверки электронных подписей и соответствующих им объектных идентификаторов, зарегистрированных в Удостоверяющем центре, приведен в Приложении № 1 к настоящему Регламенту.

13.6. Сертификат ключа проверки электронной подписи пользователя Удостоверяющего центра (клиентский сертификат) в расширении Extended Key Usage или Application Policy должен содержать, включая, но не ограничиваясь, следующие области использования:

- Пользователь Центра регистрации, HTTP, TLS client (1.2.643.2.2.34.6);
- Проверка подлинности клиента (1.3.6.5.5.7.3.2);
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4);

13.7. Сроки действия ключевых документов.

13.7.1. Сроки действия ключевых документов Уполномоченного лица Удостоверяющего центра.

13.7.1.1. Срок действия ключа электронной подписи уполномоченного лица Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности удостоверяющего центра, и для средства электронной цифровой подписи, с использованием которого данный ключ электронной подписи был сформирован.

13.7.1.2. Начало периода действия ключа электронной подписи уполномоченного лица Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

13.7.1.3. Срок действия сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра не превышает 15 (пятнадцать) лет. Дата и время начала периода действия сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра и его окончания заносится в поля «Действителен с» и «Действителен по» соответственно.

13.7.2. Сроки действия ключевых документов пользователей Удостоверяющего центра.

13.7.2.1. Срок действия ключа электронной подписи Пользователя УЦ составляет 1 (один) год.

13.7.2.2. Начало периода действия ключа электронной подписи пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

13.7.2.3. Срок действия сертификата ключа проверки электронной подписи пользователя УЦ не превышает 15 (пятнадцать) лет. Дата и время начала периода действия сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра и его окончания заносится в поля «Действителен с» и «Действителен по» соответственно.

14. Дополнительные положения.

14.1. Компрометация ключевых документов.

14.1.1. Компрометация ключевых документов уполномоченного лица Удостоверяющего центра.

14.1.1.1. В случае компрометации ключевых документов уполномоченного лица Удостоверяющего центра производится внеплановая смена ключей уполномоченного лица Удостоверяющего центра соответствии с пунктом 10.2 настоящего Регламента.

14.1.2. Компрометация ключевых документов пользователя УЦ.

14.1.2.1. Пользователь УЦ самостоятельно принимает решение о факте или возможной компрометации своего ключа электронной подписи.

14.1.2.2. В случае компрометации или угрозы компрометации ключа электронной подписи Пользователь УЦ обязан немедленно уведомить Оператора УЦ по телефону и приостановить действие сертификата, соответствующего скомпрометированному ключу электронной подписи, посредством подачи заявления на приостановление действия сертификата в устной форме.

14.1.2.3. Если в течение срока приостановления действия сертификата ключа проверки электронной подписи пользователь не предоставит заявление на возобновление действия сертификата, то Удостоверяющий центр отзывает (аннулирует) данный сертификат.

14.1.2.4. Внеплановая смена ключей электронной подписи осуществляется в соответствии с пунктом 9.2.7 настоящего Регламента.

14.2. Архивное хранение информации.

14.2.1. Архивированию подлежат следующая информация:

- реестр сертификатов;
- сертификаты пользователей УЦ;
- сертификаты уполномоченного лица Удостоверяющего центра;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- бланки сертификатов пользователей УЦ;
- заявления на регистрацию пользователей УЦ;
- заявления на изготовление сертификатов пользователей УЦ;
- заявления на аннулирование (отзыв) сертификатов;
- заявления на приостановление действия сертификатов;
- заявления на возобновление действия сертификатов;
- заявления на подтверждение подлинности электронной подписи в ЭД;
- заявления на получение информации о статусе сертификата;
- журналы учета СКЗИ;
- журналы аудита средств Удостоверяющего центра;
- служебные документы Удостоверяющего центра.

14.2.2. Источником комплектования архивного фонда являются подразделения Министерства, обеспечивающие документирование в соответствии с регламентом делопроизводства.

14.2.3. Архивные документы хранятся в специально оборудованном помещении, обеспечивающим режим хранения архивных документов.

14.2.4. Документы, подлежащие архивному хранению, хранятся в Удостоверяющем центре в течение срока деятельности Удостоверяющего центра.

14.3. Форс-мажор.

14.3.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

14.3.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) различных органов, повлекшие невозможность исполнения Стороной или Сторонами своих обязательств по настоящему Регламенту.

14.3.3. В случае возникновения форс-мажорных обстоятельств, срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

14.3.4. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

14.3.5. Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

14.3.6. В случае, если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства.

15. Список приложений.

- 15.1. Приложение № 1 Список объектных идентификаторов (OID), используемых Удостоверяющим центром Мининформполитики Чувашии при изготовлении сертификатов ключей проверки электронной подписи пользователей УЦ
- 15.2. Приложение № 2 Форма заявления о присоединении к Регламенту УЦ
- 15.3. Приложение № 3 Форма заявления на регистрацию Пользователя УЦ - Уполномоченного представителя юридического лица
- 15.4. Приложение № 4 Форма доверенности на регистрацию Пользователя УЦ - уполномоченного представителя ЮЛ
- 15.5. Приложение № 5 Заявление на изготовление сертификата Пользователя УЦ - Уполномоченного представителя ЮЛ
- 15.6. Приложение № 6 Форма доверенности на получение сертификата Пользователя УЦ - Уполномоченного представителя ЮЛ
- 15.7. Приложение № 7 Заявление на аннулирование (отзыв) сертификата Пользователя УЦ - Уполномоченного представителя ЮЛ
- 15.8. Приложение № 8 Заявление на регистрацию Пользователя УЦ – юридического лица
- 15.9. Приложение № 9 Форма доверенности на регистрацию Пользователя УЦ – юридического лица
- 15.10. Приложение № 10 Заявление на изготовление сертификата Пользователя УЦ – юридического лица
- 15.11. Приложение № 11 Форма доверенности на получение ключей проверки электронной подписи и сертификата Пользователя УЦ – юридического лица
- 15.12. Приложение № 12 Заявление на аннулирование (отзыв) сертификата Пользователя УЦ – юридического лица
- 15.13. Приложение № 13 Заявление на приостановление действия сертификата Пользователя УЦ - Уполномоченного представителя ЮЛ
- 15.14. Приложение № 14 Заявление на приостановление действия сертификата Пользователя УЦ – юридического лица
- 15.15. Приложение № 15 Заявление на возобновление действия сертификата Пользователя УЦ - Уполномоченного представителя ЮЛ
- 15.16. Приложение № 16 Заявление на возобновление действия сертификата Пользователя УЦ – юридического лица
- 15.17. Приложение № 17 Заявление на получение информации о статусе сертификата ключа проверки электронной подписи
- 15.18. Приложение № 18 Заявление подтверждение подлинности электронной подписи в электронном документе
- 15.19. Приложение № 19 Форма сертификата ключа проверки электронной подписи на бумажном носителе
- 15.20. Приложение № 20 Рекомендации по заполнению полей табличной формы заявления на регистрацию Пользователя УЦ
- 15.21. Приложение № 21 Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

Приложение № 1

Список объектных идентификаторов (OID), используемых
Удостоверяющим центром Мининформполитики Чувашии
при изготовлении сертификатов ключей проверки
электронной подписи пользователей УЦ

№	Объектный идентификатор	Область применения
1	1.2.643.5.3.21	Удостоверяющий центр Министерства информационной политики и массовых коммуникаций
2	1.2.643.5.3.21.1	Подписание документов в рамках корпоративных информационных систем органов государственной власти Чувашской Республики
2	1.2.643.5.3.21.5.1	Служба актуальных статусов сертификатов Удостоверяющего центра Мининформполитики Чувашии
2	1.2.643.5.3.21.5.2	Служба штампов времени Удостоверяющего центра Мининформполитики Чувашии
3	1.2.643.3.7.1	Подписание документов в рамках Системы «Контур-Экстерн». Подписание документов уполномоченным представителем
4	1.2.643.3.7.1.1.1	Абонент Системы Контур-Экстерн
5	1.2.643.3.7.3.15	Информационная система Диадок
6	1.2.643.7.2.21.1.2	Размещение сведений в сводном реестре
7	1.2.643.100.2.1	Доступ к СМЭВ уполномоченного лица органа государственной власти (ЭП-СП)
8	1.2.643.100.2.2	Доступ к СМЭВ (орган государственной власти) (ЭП-ОВ)
9	1.2.643.5.1.24.2.6	Руководитель органа государственной власти субъекта Российской Федерации или иное уполномоченное лицо данного органа в соответствии
10	1.2.643.5.1.24.2.19	Руководитель органа местного самоуправления или иное уполномоченное лицо данного органа в соответствии с федеральным законом
11	1.2.643.5.1.24.2.43	Руководитель территориального органа федерального органа исполнительной власти или иное уполномоченное лицо данного органа в соответствии с федеральным законом

Приложение № 2
Форма заявления о присоединении к Регламенту УЦ

Министерство информационной политики
и массовых коммуникаций Чувашской
Республики

_____ № _____

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____ (должность руководителя)

_____ (фамилия, имя, отчество руководителя)

действующего на основании _____,
присоединяется к Регламенту удостоверяющего центра Министерства информационной
политики и массовых коммуникаций Чувашской Республики, утвержденному приказом
Министерства информационной политики и массовых коммуникаций Чувашской
Республики от «____» _____ 201__ года № _____ (далее – Регламент).

Должностные лица _____,
(сокращенное наименование организации)

регистрирующиеся в Удостоверяющем центре Министерства информационной политики
и массовых коммуникаций Чувашской Республики, с Регламентом, опубликованном на
сайте Удостоверяющего центра по адресу <http://www.cap.ru/certsrv/doc/reglament.rtf>,
ознакомлены и обязуются соблюдать все его положения.

_____ / _____ /
(должность руководителя) (подпись) (расшифровка подписи)

М.П.

_____ (заполняется уполномоченным лицом Удостоверяющего центра)

Данное заявление¹ о присоединении к Регламенту зарегистрировано в реестре
удостоверяющего центра Министерства информационной политики и массовых
коммуникаций Чувашской Республики.

Регистрационный № _____ от «____» _____ 20__ г.

Уполномоченное лицо Удостоверяющего _____ / _____ /
центра (подпись) (расшифровка подписи)

М.П.

¹ Заявление о присоединении к Регламенту предоставляется в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр возвращается Заявителю.

Приложение № 3

Форма заявления на регистрацию Пользователя УЦ -
Уполномоченного представителя юридического лица

Министерство информационной
политики и массовых коммуникаций
Чувашской Республики

_____ № _____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность руководителя)

(фамилия, имя, отчество руководителя)

действующего на основании _____

просит зарегистрировать своего Уполномоченного представителя

(фамилия, имя, отчество)

в Реестре удостоверяющего центра Министерства информационной политики и массовых коммуникаций Чувашской Республики в качестве Пользователя Удостоверяющего центра, сформировать ключ проверки электронной подписи и изготовить сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	
Подразделение	
Наименование организации	
Населенный пункт	
Область	21 Чувашская Республика – Чувашия
Страна	RU
Адрес электронной почты	

ИНН организации		
ОГРН		
СНИЛС		
Области использования ключа (расширения сертификата) ¹	Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6)

Настоящим _____
(фамилия, имя, отчество Уполномоченного представителя)

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных и признает, что персональные данные, заносимые в сертификат ключа проверки электронной подписи, владельцем которых он является, относятся к общедоступным персональным данным.

С Регламентом удостоверяющего центра Министерства информационной политики и массовых коммуникаций Чувашской Республики, опубликованным на сайте Удостоверяющего центра по адресу <http://www.cap.ru/certsrv/doc/reglament.rtf>, ознакомлен и обязуюсь соблюдать все его положения.

Уполномоченный представитель,
регистрирующийся в Удостоверяющем центре

_____/_____
(подпись) (расшифровка подписи)

(должность руководителя)

_____/_____
(подпись) (расшифровка подписи)

М.П.

¹ Дополнительные области использования ключа приведены в Приложении № 1 [Регламента УЦ](#)

Приложение № 4

Форма доверенности на регистрацию Пользователя
УЦ - уполномоченного представителя ЮЛ

Доверенность

г. _____ « _____ » _____ 20__ г.

(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество доверенного лица)

(серия и номер паспорта, кем и когда выдан)

1. Предоставить в Министерство информационной политики и массовых коммуникаций Чувашской Республики необходимые документы для регистрации своего Уполномоченного представителя - Пользователя Удостоверяющего центра

(фамилия, имя, отчество Уполномоченного представителя юридического лица)

2. Получить сертификат ключа подписи Уполномоченного лица Удостоверяющего центра, сформированный ключ проверки электронной подписи и сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра, средства электронной подписи и иные документы.

Представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по « _____ » _____ 20__ г.

Подпись доверенного лица _____ / _____ подтверждаю.
(Фамилия И.О.) (подпись)

(должность руководителя)

(подпись)

(Ф.И.О.)

М.П.

Приложение № 5
Заявление на изготовление сертификата Пользователя
УЦ - Уполномоченного представителя ЮЛ

Министерство информационной
политики и массовых коммуникаций
Чувашской Республики

_____ № _____

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____ (должность руководителя)

_____, (фамилия, имя, отчество руководителя)

действующего на основании _____,

в связи с _____, (причина изготовления сертификата)

просит сформировать ключ проверки электронной подписи и изготовить сертификат ключа проверки электронной подписи своего Уполномоченного представителя – Пользователя Удостоверяющего центра

_____ (фамилия, имя, отчество Пользователя УЦ)

в соответствии с указанными в настоящем заявлении идентификационными данными¹ и областями использования ключа:

Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	
Подразделение	
Наименование организации	

¹ В таблице указываются данные, заявленные ранее при регистрации Пользователя УЦ и имеющиеся в сертификате ключа проверки электронной подписи

Город	
Область	
Страна	RU
Адрес электронной почты	
ИНН организации	
ОГРН	
СНИЛС	
Области использования ключа (расширения сертификата) ¹	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации (1.2.643.2.2.34.6)

Настоящим _____
(фамилия, имя, отчество Пользователя УЦ)

(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра

_____/_____
(подпись) (расшифровка подписи)

(должность руководителя)

_____/_____
(подпись) (расшифровка подписи)

М.П.

¹ Области использования ключа (расширения сертификата) приведены в приложении №1 [Регламента УЦ](#)

Приложение № 6

Форма доверенности на получение сертификата
Пользователя УЦ - Уполномоченного представителя ЮЛ

Доверенность

г. _____ « _____ » _____ 20__ г.

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____, (должность руководителя)

_____ (фамилия, имя, отчество руководителя)

действующего на основании _____,

уполномочивает _____ (фамилия, имя, отчество доверенного лица)

_____ (серия и номер паспорта, кем и когда выдан)

1. Предоставить в Министерство информационной политики и массовых коммуникаций Чувашской Республики необходимые документы для формирования ключа проверки электронной подписи и изготовления сертификата ключа проверки электронной подписи своего Уполномоченного представителя - Пользователя Удостоверяющего центра

_____ (фамилия, имя, отчество Пользователя УЦ)

2. Получить изготовленный для _____ (фамилия, имя, отчество Пользователя УЦ)

ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, а также сертификат ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра.

Представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по « _____ » _____ 20__ г.

Подпись доверенного лица _____ / _____ подтверждаю.
(Фамилия И.О.) (подпись)

_____ (должность руководителя организации)

_____ / _____ (подпись)

_____ / _____ (Ф.И.О.)

М.П.

Приложение № 7

Заявление на аннулирование (отзыв) сертификата
Пользователя УЦ - Уполномоченного представителя ЮЛ

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

(полное наименование организации, включая организационно-правовую форму)

В лице _____

(должность руководителя)

(фамилия, имя, отчество руководителя)

действующего на основании _____

В связи с _____

(причина отзыва сертификата)

просит аннулировать (отозвать) сертификат ключа проверки электронной подписи своего
Уполномоченного представителя – Пользователя Удостоверяющего центра

(фамилия, имя, отчество)

содержащий следующие данные¹:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	

¹ В таблице указываются данные, заявленные ранее при регистрации Пользователя УЦ и имеющиеся в сертификате ключа подписи

Подразделение	
Наименование организации	
Город	
Область	
Страна	RU
Адрес электронной почты	
ИНН организации	
ОГРН	
СНИЛС	

Владелец сертификата

_____/_____/_____
(подпись) (расшифровка подписи)

(должность руководителя)

_____/_____/_____
(подпись) (расшифровка подписи)

М.П.

Приложение № 8
Заявление на регистрацию
Пользователя УЦ – юридического лица

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____ (должность руководителя)

_____ (фамилия, имя, отчество руководителя)

действующего на основании _____,

просит зарегистрировать в Реестре Удостоверяющего центра юридическое лицо

_____ (полное или сокращенное наименование организации)

в качестве Пользователя Удостоверяющего центра, сформировать ключ проверки электронной подписи и изготовить сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	
Подразделение	
Наименование организации	
Город	
Область	21 Чувашская Республика – Чувашия
Страна	RU
Адрес электронной почты	
ИНН организации	
ОГРН	
Области использования ключа	Проверка подлинности клиента 1.3.6.1.5.5.7.3.2

(расширения сертификата) ¹	Защищенная электронная почта Пользователь Центра Регистрации	1.3.6.1.5.5.7.3.4 1.2.643.2.2.34.6
---------------------------------------	---	---------------------------------------

(должность руководителя)

_____/_____/_____
(подпись) (Ф.И.О.)

М.П.

¹ Области использования ключа (расширения сертификата) приведены в приложении №1 [Регламента УЦ](#)

Приложение № 9
Форма доверенности на регистрацию
Пользователя УЦ – юридического лица

Доверенность

Г. _____ « ____ » _____ 20__ г.

(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество доверенного лица)

(серия и номер паспорта, кем и когда выдан)

1. Предоставить в Министерство информационной политики и массовых коммуникаций Чувашской Республики необходимые документы для регистрации юридического лица

(полное или сокращенное наименование организации)

в Реестре Удостоверяющего центра в качестве Пользователя Удостоверяющего центра.

2. Получить сертификат ключа подписи Уполномоченного лица Удостоверяющего центра, сформированный ключ проверки электронной подписи и сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра, средства электронной подписи и иные документы.

Представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по « ____ » _____ 20__ г.

Подпись доверенного лица _____ / _____ подтверждаю.
(Фамилия И.О.) (подпись)

(должность руководителя)

(подпись)

(Ф.И.О.)

М.П.

Приложение № 10
Заявление на изготовление сертификата
Пользователя УЦ – юридического лица

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____ (должность руководителя)

_____ (фамилия, имя, отчество руководителя)

действующего на основании _____,

в связи с _____ (причина изготовления сертификата)

просит сформировать ключ проверки электронной подписи и изготовить сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра – юридического лица в соответствии с указанными в настоящем заявлении идентификационными данными¹ и областями использования ключа:

Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	
Подразделение	

¹ В таблице указываются данные, заявленные ранее при регистрации Пользователя УЦ и имеющиеся в сертификате ключа подписи

Наименование организации		
Город		
Область	21 Чувашская Республика – Чувашия	
Страна	RU	
Адрес электронной почты		
ИНН организации		
ОГРН		
Области использования ключа (расширения сертификата) ¹	Проверка подлинности клиента	1.3.6.1.5.5.7.3.2
	Защищенная электронная почта	1.3.6.1.5.5.7.3.4
	Пользователь Центра Регистрации	1.2.643.2.2.34.6

(должность руководителя)

_____/_____/_____
(подпись) (Ф.И.О.)

М.П.

¹ Области использования ключа (расширения сертификата) приведены в приложении №1 [Регламента УЦ](#)

Форма доверенности на получение ключей проверки электронной подписи и сертификата Пользователя УЦ – юридического лица

Доверенность

г. _____ « ____ » _____ 20__ г.

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____, (должность руководителя)

_____ (фамилия, имя, отчество руководителя)

действующего на основании _____,

уполномочивает _____ (фамилия, имя, отчество доверенного лица)

_____ (серия и номер паспорта, кем и когда выдан)

1. Предоставить в Министерство информационной политики и массовых коммуникаций Чувашской Республики необходимые документы для формирования ключей проверки электронной подписи и изготовления сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра – юридического лица

_____ (полное или сокращенное наименование организации)

2. Получить изготовленный ключ проверки электронной подписи и сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра, а также сертификат ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра.

Представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по « ____ » _____ 20__ г.

Подпись доверенного лица _____ / _____ подтверждаю.
(Фамилия И.О.) (подпись)

_____ (должность руководителя)

_____ / _____ (подпись)

_____ / _____ (Ф.И.О.)

М.П.

Приложение № 12
Заявление на аннулирование (отзыв) сертификата
Пользователя УЦ – юридического лица

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____ (должность руководителя)

_____, (фамилия, имя, отчество руководителя)

действующего на основании _____,

в связи с _____ (причина отзыва сертификата)

просит аннулировать (отозвать) сертификат ключа подписи зарегистрированного Пользователя Удостоверяющего центра – юридического лица, содержащий следующие данные¹:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	
Подразделение	
Наименование организации	

¹ В таблице указываются данные, заявленные ранее при регистрации Пользователя УЦ и имеющиеся в сертификате ключа подписи

Город	
Область	
Страна	RU
Адрес электронной почты	
ИНН организации	
ОГРН организации	

(должность руководителя)

_____ / _____ /

(подпись) (Ф.И.О.)

М.П.

Приложение № 13

Заявление на приостановление действия сертификата
Пользователя УЦ - Уполномоченного представителя ЮЛ

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

(полное наименование организации, включая организационно-правовую форму)

В лице _____

(должность руководителя)

(фамилия, имя, отчество руководителя)

действующего на основании _____

В связи с _____

(причина приостановления действия сертификата)

просит приостановить действие сертификата ключа проверки электронной подписи
Уполномоченного представителя – Пользователя Удостоверяющего центра

(фамилия, имя, отчество)

содержащий следующие данные¹:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	

¹ В таблице указываются данные, заявленные ранее при регистрации Пользователя УЦ и имеющиеся в сертификате ключа подписи

Подразделение	
Наименование организации	
Город	
Область	
Страна	RU
Адрес электронной почты	
ИНН организации	
ОГРН	
СНИЛС	

Срок приостановления действия сертификата _____ дней¹.
(количество дней прописью)

Владелец сертификата

_____/_____
(подпись) (расшифровка подписи)

(должность руководителя)

_____/_____
(подпись) (расшифровка подписи)

М.П.

¹ Срок приостановления действия сертификата должен составлять не менее десяти дней

Приложение № 14
Заявление на приостановление действия сертификата
Пользователя УЦ – юридического лица

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____ (должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____,

в связи с _____,
(причина приостановления действия сертификата)

просит приостановить действие сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра – юридического лица, содержащий следующие
данные¹:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	
Подразделение	
Наименование организации	

¹ В таблице указываются данные, заявленные ранее при регистрации Пользователя УЦ и имеющиеся в сертификате ключа подписи

Город	
Область	
Страна	RU
Адрес электронной почты	
ИНН организации	
ОГРН организации	

Срок приостановления действия сертификата _____ дней¹.
(количество дней прописью)

(должность руководителя)

_____/_____
(подпись) (Ф.И.О.)

М.П.

¹ Срок приостановления действия сертификата должен составлять не менее десяти дней

Приложение № 15

Заявление на возобновление действия сертификата
Пользователя УЦ - Уполномоченного представителя ЮЛ

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

(полное наименование организации, включая организационно-правовую форму)

В лице _____

(должность руководителя)

(фамилия, имя, отчество руководителя)

действующего на основании _____

В связи с _____

(причина возобновления действия сертификата)

просит возобновить действие сертификата ключа проверки электронной подписи
Уполномоченного представителя – Пользователя Удостоверяющего центра

(фамилия, имя, отчество)

содержащий следующие данные¹:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
Должность	

¹ В таблице указываются данные, заявленные ранее при регистрации Пользователя УЦ и имеющиеся в сертификате ключа подписи

Название улицы, номер дома	
Подразделение	
Наименование организации	
Город	
Область	
Страна	RU
Адрес электронной почты	
ИНН организации	
ОГРН	
СНИЛС	

Владелец сертификата

_____/_____/_____
(подпись) (расшифровка подписи)

(должность руководителя)

_____/_____/_____
(подпись) (расшифровка подписи)

М.П.

Приложение № 16
Заявление на возобновление действия сертификата
Пользователя УЦ – юридического лица

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____ (должность руководителя)

_____ (фамилия, имя, отчество руководителя),

действующего на основании _____,

в связи с _____ (причина возобновления действия сертификата)

просит возобновить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра – юридического лица, содержащий следующие данные¹:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	
Подразделение	
Наименование организации	

¹ В таблице указываются данные, заявленные ранее при регистрации Пользователя УЦ и имеющиеся в сертификате ключа подписи

Город	
Область	
Страна	RU
Адрес электронной почты	
ИНН организации	
ОГРН организации	

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

(должность руководителя)

_____/_____
(подпись) (Ф.И.О.)

М.П.

Приложение № 17
Заявление на получение информации о статусе
сертификата ключа проверки электронной подписи

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

_____ № _____

_____ (полное наименование организации, включая организационно-правовую форму)

В лице _____
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____,

В связи с _____,
(причина запроса информации о статусе сертификата)

просит предоставить информацию о статусе сертификата ключа проверки электронной подписи, содержащий следующие данные¹:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
Должность	
Название улицы, номер дома	
Подразделение	
Наименование организации	
Город	

¹ В таблице указываются данные, имеющиеся в сертификате, информация о статусе которого запрашивается

Министерство информационной
политики и массовых
коммуникаций Чувашской
Республики

М.П.

Приложение № 19
Форма сертификата ключа проверки электронной
подписи на бумажном носителе

Удостоверяющий центр Министерства информационной политики и массовых
коммуникаций Чувашской Республики
Бланк сертификата ключа проверки электронной подписи

Сведения о сертификате:**Кому выдан:**

Наименование организации

Кем выдан:

CASCCL

Действителен с 22 ноября 2012 г. 10:16:00 UTC по 22 ноября 2013 г. 10:26:00 UTC

Версия: 3 (0x2)**Серийный номер:** 61A3 239A 0001 0000 1E93**Издатель сертификата:** CN = УЦ ОИВ Чувашии, OU = Подразделение, O = Мининформполитики Чувашии, L = Чебоксары, S = 21 Чувашская Республика - Чувашия, C = RU, E = certadmin@cap.ru, STREET = Президентский бульвар, 10, ИНН = 002130106185, ОГРН = 1122130008791**Срок действия:**

Действителен с: 22 ноября 2012 г. 10:16:00 UTC

Действителен по: 22 ноября 2013 г. 10:26:00 UTC

Владелец сертификата: SN = Фамилия, G = Имя Отчество, T = Должность, STREET = Улица, дом, Неструктурированный адрес = Местонахождение организации, CN = Наименование организации, OU = Подразделение, O = Наименование организации, L = Город, S = Область, C = RU, E = aaa@bb.cap.ru, ИНН = 001234567890, ОГРН = 1234567890123, СНИЛС = 12345678901**Открытый ключ:**

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.19

Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01

Значение: 0440 C78C FA41 9BD4 F82A 8E5C FF82 CFF4 23A6 D17F CFE9 BA1D 01BF 0429 AF9D 201D 27BC E6B7 13C3 BC5F EA35 F52C 5172 5837 1B5C E8D3 2BC0 5B07 4A6F EBD7 9E88 A0D3 8DC4

Расширения сертификата X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

2. Расширение 1.2.840.113549.1.9.15

Название: Возможности SMIME

Значение: [1]Возможности SMIME Идентификатор объекта=1.2.643.2.2.21

3. Расширение 2.5.29.37

Название: Улучшенный ключ

Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

4. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: 97 e5 79 d5 4c c6 87 b8 bd dd 31 8a 29 d3 5c 47 c5 84 9d 17

5. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение: Идентификатор ключа=d7 64 50 0c e4 42 0a 6b a3 cd 12 d3 bf c1 2e ec e9 f8 6f c5

6. Расширение 2.5.29.31

Название: Точки распространения списков отзыва (CRL)

Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя:

URL=http://www.cap.ru/certsrv/certenroll/CASCCL_2011.crl URL=http://ra.cap.ru/RA/CDP/d764500cc4420a6ba3cd12d3bfc12eece9f86fc5.crl

7. Расширение 1.3.6.1.5.5.7.1.1

Название: Доступ к информации о центрах сертификации

Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1)

Дополнительное имя: URL=http://ocsp.cap.ru/ocsp/ocsp.srf [2]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://www.cap.ru/certsrv/certenroll/CASCCL_2011.crt

8. Расширение 2.5.29.32

Название: Политики сертификата

Значение: [1]Политика сертификата: Идентификатор политики=Класс средств УЦ KC2 [2]Политика сертификата: Идентификатор политики=Класс

средства ЭП KC1 [3]Политика сертификата: Идентификатор политики=Класс средства ЭП KC2 [4]Политика сертификата: Идентификатор

политики=Средства ЭП УЦ: КриптоПро CSP 2.0 (СФ/114-1479 от 05.06.2010). КриптоПро УЦ 1.5 (СФ/128-1657 от 01.05.2011) [5]Политика сертификата:

Идентификатор политики=Средство ЭП владельца: КриптоПро CSP 3.6

Подпись Удостоверяющего центра:

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-2001

Идентификатор: 1.2.643.2.2.3

Параметры: 05 00

Значение: 60F9 D4DC AD71 FEA6 0B67 7091 E285 A16B D3B4 4833 877C 8B3B AF09 EB11 787C 18D0 9864 AD70 BF58 102D DC41 B0B8 C22F 695F 11D2 2093 E101 1523 6C4C 6220 B763 A157

Подпись владельца сертификата: _____ / _____

" ____ " _____ 20__ г.
М. П.

Уполномоченное лицо Удостоверяющего Центра: _____ / _____

" ____ " _____ 20__ г.
М. П.

Приложение № 20
Рекомендации по заполнению полей табличной
формы заявления на регистрацию Пользователя УЦ

1. Общие положения.

1.1. Настоящие Рекомендации описывает правила заполнения полей табличной формы заявления на регистрацию Пользователя УЦ для включения информации в сертификат, формируемый Удостоверяющим центром при регистрации Пользователя УЦ.

1.2. Настоящие Рекомендации предназначены для их использования при составлении заявлений на регистрацию пользователей Удостоверяющего центра, предоставляемых Заявителями.

1.3. Операторы УЦ руководствуются настоящими Рекомендациями при регистрации пользователей Удостоверяющего центра и изготовлении сертификатов ключей проверки электронной подписи.

1.4. Данный документ разработан на основании следующих нормативно-правовых актов и документов:

- Федерального закона «Об электронной подписи»;
- Приказа ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
- Методических рекомендаций по составу квалифицированного сертификата ключа проверки электронной подписи, опубликованных на сайте <http://smev.gosuslugi.ru/portal/>;
- Методических рекомендаций по использованию электронной подписи при межведомственном электронном взаимодействии, опубликованных на сайте <http://smev.gosuslugi.ru/portal/>

1.5. Используемые сокращения:

ИНН – индивидуальный номер налогоплательщика.

ОГРН – основной государственный регистрационный номер.

ФИО – фамилия имя отчество.

ФЛ – физическое лицо.

ЮЛ – юридическое лицо.

2. Виды сертификатов.

2.1. Удостоверяющий центр осуществляет изготовление ключей электронной подписи и сертификатов ключей проверки электронной подписи:

- юридических лиц;
- должностных лиц - физических лиц, которые являются Уполномоченными представителями юридических лиц (должностные лица участников электронного взаимодействия корпоративных информационных систем органов государственной власти Чувашской Республики);
- корпоративных информационных систем органов государственной власти Чувашской Республики.

2.1.1. Ключи электронной подписи должностного лица предназначены для подписания электронных документов от имени конкретного сотрудника – физического лица;

2.1.2. Ключи электронной подписи юридического лица предназначены для подписания электронных документов от имени юридического лица.

2.1.3. Ключи электронной подписи информационных систем предназначены для автоматического формирования электронной подписи от имени информационной системы.

2.2. В зависимости от требуемого вида сертификата Заявитель оформляет заявление на регистрацию Пользователя УЦ и предоставляет в Удостоверяющий центр информацию, необходимую для изготовления сертификата.

3. Состав полей сертификата.

Обозначение	Общее имя	Макс. длина	Значение	Формат
CN	Общее имя	64	В зависимости от назначения сертификата: - наименование организации; - название информационной системы	Раздел 5 Раздел 6 Раздел 7
O	Организация	64	Полное или сокращенное наименование организации согласно учредительным документам	Раздел 6
OU	Подразделение	64	Наименование подразделения организации согласно штатному расписанию	Раздел 8
T	Должность	64	Наименование замещаемой должности	Раздел 9
S	Регион	128	Для организаций Чувашской Республики указывается: 21 Чувашская Республика - Чувашия	Раздел 10
L	Населенный пункт	128	Наименование населенного пункта, в котором располагается организация	
E	Адрес электронной почты	128	Адрес электронной почты	
C	Страна	2	RU	
OGRN	ОГРН	13	ОГРН организации	Раздел 11
INN	ИНН	12	ИНН организации	Раздел 12
SNILS	СНИЛС	11	СНИЛС должностного лица	Раздел 13
UnstructuredAddress, StreetAddress	Название улицы, номер дома	1024	Наименование улицы и номер дома в соответствии с учредительными документами (согласно данным из Устава, Положения, выписки из ЕГРЮЛ), либо полный адрес местонахождения организации	

4. Общие требования к заполнению полей.

4.1. Не разрешается использовать пробел в начале и в конце текста.

4.2. Каждое слово в тексте должно быть отделено 1 пробелом.

4.3. Перечень допустимых символов приведен в разделе 10.

4.4. Символы, дополнительно приведенные в разделе 10, разрешается использовать только в том случае, если они встречаются внутри официальных названий, указанных в документах.

4.5. В полях наименования организации, информационной системы, подразделения организации, должности, адреса организации разрешается использование символов из набора (Раздел 10). При этом, следующие символы разрешается использовать только в том случае, если они встречаются внутри официальных названий:

№	Символ	Название
---	--------	----------

№	Символ	Название
1	'	апостроф
2	«	двойная левая угловая кавычка
3	»	двойная правая угловая кавычка

5. Формат ФИО.

5.1. ФИО должно быть указано полностью так, как оно указано в основном документе, удостоверяющем личность владельца.

5.2. Если в фамилии, имени или отчестве в написании присутствует «дефис», то в сертификат так и вносится с дефисом без пробелов (например: Салтыков-Щедрин).

5.3. Если фамилия, имя или отчество состоит из нескольких слов разделенных пробелом, то в сертификат вносится одним словом, части которого соединены «подчеркиванием» без пробелов (например: фамилия «Ван Чо» будет записана Ван_Чо).

5.4. Разрешается использование символов из раздела 10, за исключением символов:

Символ	Название	Символ	Название
"	универсальная кавычка	+	знак плюс
%	процент	«	двойная левая угловая кавычка
&	амперсанд	№	знак номер
'	апостроф	»	двойная правая угловая кавычка

6. Формат наименования организации.

6.1. Наименование организации указывается в соответствии с учредительными документами (устава, положения, выписки из ЕГРЮЛ).

6.2. В случае, если полное официальное наименование организации превышает 64 символа, допускается использовать официальное сокращенное наименование организации.

7. Формат наименования информационной системы.

7.1. Наименование информационной (автоматизированной) системы указывается в соответствии с официальным наименованием информационной системы согласно техническому паспорту или иному документу на информационную систему.

7.2. В случае, если полное официальное наименование информационной системы превышает 64 символа, допускается использовать официальное сокращенное наименование информационной системы.

8. Формат наименования подразделения организации.

8.1. Наименование подразделения организации указывается согласно штатному расписанию организации.

8.2. В случае, если полное официальное наименование подразделения организации превышает 64 символа, допускается использовать официальное сокращенное наименование подразделения организации.

9. Формат должности.

9.1. Наименование должности указывается согласно штатному расписанию, приказу (распоряжению) о назначении на должность или иному документу организации.

10. Формат наименования субъекта РФ

- 10.1. Первое слово – номер региона, 2 цифры, лидирующий ноль указывать обязательно.
- 10.2. Остальной текст – название региона с заглавной буквы.
- 10.3. Для организаций Чувашской Республики наименование субъекта РФ указывается: 21 Чувашская Республика – Чувашия.

11. Формат ОГРН

- 11.1. Текст длиной 13 цифр.
- 11.2. ОГРН юридического лица должен присутствовать всегда.

12. Формат ИНН

- 12.1. Текст длиной 12 цифр.
- 12.2. Должен содержать два лидирующих нуля, например «007707049388».
- 12.3. ИНН должен присутствовать всегда.

13. Формат СНИЛС

- 13.1. Текст длиной 11 цифр.
- 13.2. Не заполняется при создании сертификата на информационную систему.

14. Перечень допустимых символов

Кроме цифр, символов латинского и кириллического алфавита, допустимо использовать следующие символы:

Символ	Название	Символ	Название
	пробел	-	Дефис
"	универсальная кавычка	.	Точка
%	процент	:	Двоеточие
&	амперсанд	;	точка с запятой
'	апостроф	@	коммерческое АТ, «собака»
(	левая скобка	—	Подчеркивание
)	правая скобка	«	двойная левая угловая кавычка
+	знак плюс	№	знак номер
,	запятая	»	двойная правая угловая кавычка

15. Примеры заполнения полей табличной формы заявления на регистрацию.

15.1. Для должностного лица.

Фамилия	Иванов
Имя Отчество	Иван Иванович
Должность	Начальник отдела

Название улицы, номер дома	Президентский бульвар, 10	
Подразделение	Отдел администрирования	
Наименование организации	Мининформполитики Чувашии	
Город	Чебоксары	
Область	21 Чувашская Республика – Чувашия	
Страна	RU	
Адрес электронной почты	info@cap.ru	
ИНН организации	001234567891	
ОГРН организации	0123456789123	
СНИЛС	12345678901	
Расширения сертификата	Проверка подлинности клиента	(1.3.6.1.5.5.7.3.2)
	Защищенная электронная почта	(1.3.6.1.5.5.7.3.4)
	Пользователь Центра Регистрации	(1.2.643.2.2.34.6)

15.2. Для юридического лица.

Фамилия	Иванов	
Имя Отчество	Иван Иванович	
Должность	Начальник отдела	
Название улицы, номер дома	Президентский бульвар, 10	
Подразделение	Отдел администрирования	
Наименование организации	Мининформполитики Чувашии	
Город	Чебоксары	
Область	21 Чувашская Республика – Чувашия	
Страна	RU	
Адрес электронной почты	info@cap.ru	
ИНН организации	001234567891	
ОГРН организации	0123456789123	
Расширения сертификата	Проверка подлинности клиента	1.3.6.1.5.5.7.3.2
	Защищенная электронная почта	1.3.6.1.5.5.7.3.4
	Пользователь Центра Регистрации	1.2.643.2.2.34.6

15.3. Для информационной системы.

Общее имя	ИС СЭД ОГВ Чувашии	
Название улицы, номер дома	Президентский бульвар, 10	
Наименование организации	Мининформполитики Чувашии	
Город	Чебоксары	
Область	21 Чувашская Республика – Чувашия	
Страна	RU	
Адрес электронной почты	info@cap.ru	
ИНН организации	001234567891	
ОГРН организации	0123456789123	
Расширения сертификата	Проверка подлинности клиента	1.3.6.1.5.5.7.3.2
	Защищенная электронная почта	1.3.6.1.5.5.7.3.4
	Пользователь Центра Регистрации	1.2.643.2.2.34.6

Приложение № 21
Руководство по обеспечению безопасности
использования электронной подписи и средств
электронной подписи

1. Общие принципы обеспечения информационной безопасности при организации
электронного взаимодействия с использованием электронной подписи

Организация электронного взаимодействия с использованием электронной подписи должна осуществляться с учетом требований федеральных законов «Об электронной подписи», «Об информации, информационных технологиях и о защите информации», Постановления Правительства Российской Федерации «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» от 9 февраля 2012 года № 111, Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ №152), других федеральных законов и нормативных правовых актов, осуществляющих правовое регулирование отношений в области обеспечения защиты информации и использования электронной подписи, руководящих документов ФСТЭК России и ФСБ России, эксплуатационной и технической документации на используемые средства электронной подписи, средства криптографической защиты информации (далее - СКЗИ).

Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Риски, связанные с использованием электронной подписи и средств электронной
подписи

В случае, если электронное взаимодействие с использованием электронной подписи осуществляется без учета требований нормативных правовых актов, регулирующих отношения в области использования электронных подписей, могут возникнуть или существенно возрасти риски, связанные с использованием электронной подписи, основными из которых могут являться:

- риски, связанные с проверкой принадлежности ключа электронной подписи, с помощью которой подписан электронный документ, Владелец сертификата. Лицо, владеющее сертификатом ключа проверки электронной подписи и соответствующим ему ключом электронной подписи, которым был подписан электронный документ, может заявить о том, что электронная подпись, содержащаяся в электронном документе, создана с использованием ключа электронной подписи, который не принадлежит данному Владелец сертификата;

- риски, связанные с внесенными в электронный документ изменениями, произведенными после его подписания. Лицо, ключом электронной подписи которого был подписан электронный документ, может заявить о том, что содержание документа было изменено и не соответствует содержанию документа, подписанному данным лицом;

- риски, связанные с признанием электронного документа, содержащего электронную подпись. Одна из сторон может заявить о том, что подписанный электронной подписью документ не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;

- риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае, если порядок использования электронной подписи и средств электронной подписи не соответствует требованиям нормативных правовых актов Российской Федерации, осуществляющих правовое регулирование отношений в использовании электронной подписи или не соответствует порядку использования электронной подписи, определяемому соглашениями сторон, юридическая значимость подписанных электронной подписью документов может быть поставлена под сомнение;

- риски, связанные с нарушением конфиденциальности ключей электронной подписи (использование ключей электронной подписи без согласия владельца). В случае нарушения конфиденциальности ключей электронной подписи, в том числе компрометации ключей, несанкционированного доступа к ключевым носителям или средствам электронной подписи, может быть принят в исполнение подписанный электронной подписью документ, порождающий юридически значимые последствия и исходящий от имени лица, ключ которого был скомпрометирован;

- риски, связанные с несовместимостью средств электронной подписи, используемых сторонами для организации электронного взаимодействия. Несовместимость средств электронной подписи, протоколов и форматов данных, используемых сторонами для организации электронного взаимодействия, может привести к невозможности проверки электронной подписи или к её некорректной проверке;

- риски, связанные с определением полномочий лица, подписавшего электронной подписью документ. В случае, если участниками межведомственного электронного взаимодействия не определены лица, участвующие в электронном взаимодействии, полномочия данных лиц по подписанию электронных документов от имени участника межведомственного электронного взаимодействия, а также в случае, если полномочия лица по подписанию электронных документов прекращены, одна из сторон может заявить, что полученный электронный документ содержит электронную подпись лица, не уполномоченного на подписание данного документа и не может быть принят в исполнение;

- риски, связанные с использованием сертификатов ключей электронной подписи и ключей электронной подписи, прекративших своё действие. В случае использования для подписания электронных документов ключа электронной подписи, прекратившего своё действие на момент подписания, либо, если момент подписания электронного документа не определен, использования сертификата ключа проверки электронной подписи, недействительного на день проверки электронной подписи, сторона, получившая подписанный электронной подписью документ, может заявить о непризнании такого документа юридически значимым.

В целях минимизации и исключения вышеуказанных рисков участникам электронного взаимодействия необходимо предусмотреть обеспечение комплекса правовых и организационно-технических мероприятий по обеспечению информационной безопасности при осуществлении электронного взаимодействия с использованием электронной подписи и средств электронной подписи.

Электронное взаимодействие с использованием электронной подписи, осуществляемое с учетом требований Федерального закона «Об электронной подписи», других федеральных законов, принимаемых в соответствии с ними нормативных правовых актов, регулирующих отношения в области использования электронных подписей, позволяет обеспечить:

- неотказуемость от электронного документа, содержащего электронную подпись. Электронная подпись позволяет определить лицо, подписавшее электронный документ;
- целостность электронного документа. Электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания.

В случае необходимости обеспечения конфиденциальности передаваемой информации ключи электронной подписи и СКЗИ могут использоваться для шифрования электронных документов или для организации передачи данных по защищенным каналам связи.

Средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральными законом «Об электронной подписи», позволяют:

- установить факт изменения подписанного электронного документа после момента его подписания;
- обеспечить практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

При создании электронной подписи средства электронной подписи:

- показывают лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
- создают электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;
- однозначно показывают, что электронная подпись создана.

При проверке электронной подписи средства электронной подписи:

- показывают содержание электронного документа, подписанного электронной подписью;
- показывают информацию о внесении изменений в подписанный электронной подписью электронный документ;
- указывают на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Одной из составных частей инфраструктуры открытых ключей и системы криптографической защиты информации является удостоверяющий центр, выполняющий функции по изготовлению и обслуживанию сертификатов ключей проверки электронных подписей, используемых участниками электронного взаимодействия.

Удостоверяющий центр осуществляет свою деятельность в строгом соответствии с нормативными правовыми актами Российской Федерации, руководящими документами, эксплуатационной документацией на используемые средства, Регламентом Удостоверяющего центра и другими документами, регулирующими вопросы использования электронной подписи.

Сертификаты ключей проверки электронных подписей, изготавливаемые Удостоверяющим центром, заверяются электронной подписью уполномоченного лица удостоверяющего центра, что подтверждает факт принадлежности ключа электронной подписи конкретному лицу участника электронного взаимодействия. Использование сертификатов позволяет участника электронного взаимодействия идентифицировать лицо, подписавшее электронной подписью документ, а также позволяет подтвердить целостность (неизменность) содержания подписанного электронного документа при проверке электронной подписи. Таким образом, при соблюдении требований нормативных правовых актов, регулирующих отношения в области использования электронных подписей, исключаются риски, связанные с подтверждением подлинности и отказом от содержимого документа и исключаются риски, связанные с юридической значимостью электронных документов.

3. Требования и рекомендации по обеспечению информационной безопасности при использовании средств электронной подписи

В организации, эксплуатирующей средства электронной подписи (СКЗИ), должны быть предусмотрены организационные и организационно-технические мероприятия, направленные на обеспечение информационной безопасности при использовании средств электронной подписи и определяющие требования к ответственным лицам, автоматизированным рабочим местам пользователей (далее также - АРМ), системному и прикладному программному обеспечению, условиям хранения и использования средств электронной подписи, ключей электронной подписи и ключевых носителей.

3.1. Требования и рекомендации по назначению ответственных лиц.

В организации должны быть определены лица, наделенные полномочиями по подписанию электронных документов электронной подписью, лица, ответственные за осуществление электронного взаимодействия с использованием электронной подписи и имеющих доступ к ключевым носителям, а также лица, ответственные за организацию работ по защите информации и соблюдению условий хранения и использования ключей электронной подписи и средств электронной подписи.

К работе со средствами электронной подписи должны допускаться лица, прошедшие соответствующее обучение и ознакомленные с Инструкцией ФАПСИ №152, другими нормативными правовыми актами и руководящими документами, в том числе внутренними организационными документами и инструкциями по защите информации и использованию электронной подписи, а также эксплуатационной документацией на используемые средства электронной подписи и Регламентом Удостоверяющего центра.

В организации, эксплуатирующей СКЗИ, должен быть назначен администратор информационной безопасности, на которого возлагаются задачи организации работ по защите информации, подготовки соответствующих инструкций, обучения и инструктажа пользователей, ведению журналов учета СКЗИ, настройке системного, прикладного программного обеспечения, СКЗИ и средств защиты от несанкционированного доступа, устанавливаемого на АРМ пользователей, контролю за соблюдением требований по безопасности, а также взаимодействия с удостоверяющим центром по вопросам использования электронной подписи.

3.2. Требования и рекомендации к помещениям и размещению технических средств АРМ.

Помещения, в которых расположены АРМ, предназначенные для работы со средствами электронной подписи (далее – спецпомещения), должны соответствовать требованиям Инструкции ФАПСИ №152. Должен быть исключен бесконтрольный допуск лиц, не допущенных к работе в указанных спецпомещениях. В случае необходимости присутствия посторонних лиц в спецпомещениях должен быть обеспечен контроль за их действиями.

Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Размещение АРМ должно производиться с учетом размеров контролируемой зоны и исключать возможность просмотра посторонними лицами работ, осуществляемых на АРМ.

Спецпомещения рекомендуется оснащать охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

3.3. Требования и рекомендации к АРМ пользователей.

Не допускается оставлять без контроля АРМ при включенном питании и подключенными ключевыми носителями. Перед уходом пользователь должен выключить АРМ либо заблокировать рабочую станцию с использованием средств защиты информации от несанкционированного доступа или с использованием средств операционной системы. Рекомендуется настроить автоматическое включение экранной заставки, защищенной паролем.

На АРМ пользователей рекомендуется установить сертифицированные средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД), такими как электронный замок «Соболь», СЗИ от НСД Secret Net, КСЗИ «Панцирь-К», либо других аналогичных средств защиты, а также сертифицированным антивирусным программным обеспечением.

В целях исключения возможности несанкционированного изменения аппаратной части системного блока администратору рекомендуется предусмотреть печатывание системного блока АРМ.

Необходимо предусмотреть организацию парольной защиты при включении АРМ и загрузке операционной системы с использованием СЗИ от НСД (средств доверенной загрузки), либо средств BIOS и средств операционной системы (далее также – ОС), также рекомендуется определить установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске, отключить возможность загрузки с внешних съемных дисков, привода CD-ROM, исключить нестандартные виды загрузки ОС, включая сетевую загрузку.

3.4. Требования и рекомендации по настройке системного и прикладного программного обеспечения.

На технических средствах АРМ с установленными средствами электронной подписи необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников. Не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

Не допускается установка на АРМ средств разработки и отладки программного обеспечения. Необходимо исключить возможность установки средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также вредоносного программного обеспечения, позволяющего несанкционированно получать привилегии администратора.

Рекомендуется ограничить возможности пользователя запуском только тех приложений, которые разрешены администратором безопасности.

Необходимо регулярно отслеживать и устанавливать обновления безопасности для программного обеспечения АРМ (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.4.1. Настройка операционной системы АРМ.

До начала использования средств электронной подписи администратор информационной безопасности должен произвести настройку операционной системы, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль настроек в соответствии со следующими рекомендациями:

- правом установки и настройки ОС и средств электронной подписи должен обладать только администратор безопасности;
- в целях возможности разграничения прав доступа рекомендуется использовать средства, входящие в состав СЗИ от НСД, для работы ОС рекомендуется использование файловой системы NTFS;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для работы права;
- все привилегии группы Everyone должны быть удалены;

- необходимо исключить использование режима автоматического входа пользователя в операционную систему при ее загрузке без ввода пароля;
- рекомендуется переименовать стандартную учетную запись Administrator;
- рекомендуется отключить учетная запись для гостевого входа Guest;
- исключить возможность удаленного управления, администрирования и модификации ОС и её настроек, системного реестра, для всех, включая группу Administrators;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, службы, сервисы и т.п.);
- должно быть исключено или ограничено использование пользователями сервиса Scheduler (планировщик задач). При использовании данного сервиса состав запускаемого программного обеспечения на АРМ согласовывается с администратором информационной безопасности;
- рекомендуется организовать удаление временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы средств электронной подписи. Если это невыполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
- должны быть отключены средства удаленного администрирования, в т.ч. подключение к рабочему столу с использованием службы терминалов, в случае если такое подключение осуществляется без использования защищенных каналов связи;
- должны быть установлены ограничения на доступ пользователей к системному реестру путем настройки прав доступа к системному реестру;
- на все директории, содержащие системные файлы Windows и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме администратора (Administrator), создателя/владельца (Creator/Owner) и системы (System);
- необходимо обеспечить ведение журналов аудита в ОС, при этом она должна быть настроена на завершение работы при переполнении журналов;
- настройка параметров системного реестра производится в соответствии с эксплуатационной документацией на средства электронной подписи.

3.4.2. Требования и рекомендации при организации парольной защиты.

Рекомендуется разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать правила формирования и хранения паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 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;
- пользователь должен обеспечивать конфиденциальность паролей, не допускается хранить записанные пароли в легкодоступных местах;
- периодичность смены пароля определяется принятой политикой безопасности (инструкцией по организации парольной защиты), но не должна превышать 6 месяцев.
- указанная политика должна применяться для всех учетных записей пользователей, зарегистрированных в операционной системе.

3.4.3. Установка и настройка средств электронной подписи.

Установка и настройка средств электронной подписи (СКЗИ) должна выполняться администратором информационной безопасности либо лицом, ответственным за работоспособность АРМ и прошедшим соответствующее обучение.

Установка средств электронной подписи должна производиться только с дистрибутива, полученного по доверенному каналу, в соответствии с эксплуатационной документацией на средства электронной подписи.

При установке средств электронной подписи должен быть обеспечен контроль целостности устанавливаемого программного обеспечения.

Перед установкой средств электронной подписи необходимо произвести проверку ОС на отсутствие вредоносных программ с помощью антивирусных средств.

После завершения установки осуществляются настройка и контроль работоспособности средств электронной подписи.

3.5. Подключение АРМ к сетям общего пользования.

Не рекомендуется подключать к сетям общего пользования АРМ пользователя средств электронной подписи. В случае необходимости подключения АРМ к сетям связи общего пользования такое подключение рекомендуется производить с использованием сертифицированного межсетевого экрана.

В случае подключения АРМ с установленными средствами электронной подписи к общедоступным сетям передачи данных необходимо ограничить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX и т.д.), полученных из сетей общего пользования, без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносных программ.

3.6. Обращение с ключевыми носителями.

В организации должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации, который должен исключать возможность несанкционированного доступа к ним.

Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

В качестве ключевых носителей рекомендуется использовать сертифицированные USB-ключи и смарт-карты (например eToken, ruToken)

Запрещается:

- выполнять копирование информации с ключевых носителей, которое несанкционированно администратором информационной безопасности;
- знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным;
- устанавливать ключевой носитель в другие ПЭВМ, не предназначенные для работы с ключевой информацией;
- записывать на ключевой носитель постороннюю информацию;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации с использованием средств электронной подписи либо средств, гарантирующих практическую невозможность восстановления информации с ключевых носителей.

Владелец сертификата обязан:

- хранить в тайне ключ электронной подписи;
- немедленно обратиться в удостоверяющий центр для приостановления действия сертификата ключа проверки электронной подписи или его отзыва в случае компрометации ключа электронной подписи или при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

- не использовать ключ проверки электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который отозван или действие которого приостановлено.

3.7. Учет и контроль.

Действия, связанные с хранением и эксплуатацией средств электронной подписи и ключей электронной подписи, должны фиксироваться в журналах поэкземплярного учета, ведение которого осуществляется администратором информационной безопасности в соответствии с Инструкцией ФАПСИ № 152

Администратор информационной безопасности должен периодически, не реже одного раза в два месяца, проводить проверку установленного программного обеспечения, журналов аудита операционной системы и средств защиты информации на всех АРМ пользователей, осуществлять контроль за условиями использования и хранения ключевых носителей, а также проводить периодическое тестирование технических и программных средств защиты информации.

В случае обнаружения постороннего программного обеспечения, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией, назначенной руководителем организации, а также организованы работы по анализу и устранению выявленных нарушений.