МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ

П Р И К А З

30.09.2011 г. Москва № 554

Об Удостоверяющем центре электронной подписи Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий

В соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[1] и постановлением Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия»[2] п р и к а з ы в а ю:

1. Возложить на Национальный центр управления в кризисных ситуациях МЧС России функции Удостоверяющего центра электронной подписи Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее - Удостоверяющий центр МЧС России).
2. Утвердить прилагаемый Регламент Удостоверяющего центра МЧС России.

Министр С.К. Шойгу

[1] Собрание законодательства Российской Федерации; 2011, № 15, ст. 2036, № 27 ст. 3880.
[2] Собрание законодательства Российской Федерации 2010, № 38, ст. 4823, № 24, ст. 3503.

066251

Приложение
к приказу МЧС России
от 30.09.2011 № 557

РЕГЛАМЕНТ
Удостоверяющего центра электронной подписи Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий

1. Общие положения

1.1. Предмет Регламента

Регламент Удостоверяющего Центра электронной подписи Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее Регламент) определяет условия и порядок использования электронной подписи, а так же права, обязанности, ответственность, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение его работы.

Настоящий Регламент дает право начальнику Национального центра управления в кризисных ситуациях (далее – Национальный центр МЧС России):

создавать сертификаты ключей проверки электронной подписи;

устанавливать сроки действия сертификатов;

создавать ключи электронной подписи и сертификаты пользователей;

по согласованию с Управлением защиты информации и обеспечения безопасности спасательных работ выдавать средства электронной подписи, ключи, сертификаты пользователям;

назначать доверенное лицо, администраторов и операторов Удостоверяющего центра электронной подписи Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее - Удостоверяющий центр МЧС России);

разрабатывать и утверждать документы регламентирующие работу Удостоверяющего центра МЧС России;

осуществлять закупку, дооснащение, обслуживание и ремонт оборудования Удостоверяющего центра МЧС России.

1.2. Действие Регламента

Нормы, содержащиеся в Регламенте, становятся обязательными для пользователей Удостоверяющего центра МЧС России с момента передачи ему заявления на получение сертификата ключа проверки электронной подписи (далее – Сертификат).

2. Права и обязанности сторон

2.1. Удостоверяющий центр имеет право:

отказать в аннулировании (отзыве) Сертификата пользователя Удостоверяющего центра МЧС России в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату;

отказать в приостановлении действия Сертификата пользователя Удостоверяющего центра МЧС России в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату;

отказать в возобновлении действия Сертификата пользователя Удостоверяющего центра МЧС России в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату;

аннулировать (отозвать) Сертификат пользователя Удостоверяющего центра МЧС России в случае установленного факта компрометации соответствующего закрытого ключа, с уведомлением системы услуг и владельца аннулированного (отозванного) Сертификата и указанием обоснованных причин;

приостановить действие Сертификата пользователя Удостоверяющего центра МЧС России с уведомлением системы услуг и владельца Сертификата, действие которого приостановлено, и указанием обоснованных причин;

отказать в изготовлении Сертификата пользователя Удостоверяющего центра МЧС России в случае, если использованное пользователем для формирования запроса на Сертификат средство криптографической защиты информации не поддерживается Удостоверяющим центром МЧС России.

2.2. Пользователь Удостоверяющего центра МЧС России имеет право:

получить список отозванных Сертификатов, изготовленный Удостоверяющим центром МЧС России;

получить Сертификат уполномоченного лица Удостоверяющего центра МЧС России;

применять Сертификат уполномоченного лица Удостоверяющего центра МЧС России для проверки квалифицированной электронной подписи уполномоченного лица Удостоверяющего центра МЧС России в Сертификатах, изготовленных Удостоверяющим центром МЧС России;

применять Сертификат пользователя Удостоверяющего центра МЧС России для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в Сертификате;

применять список отозванных Сертификатов, изготовленный Удостоверяющим центром МЧС России, для проверки статуса Сертификатов;

обратиться в систему услуг, пользователем которой он является, за подтверждением подлинности квалифицированных электронных подписей в электронных документах;

обратиться в систему услуг, пользователем которой он является, за подтверждением подлинности квалифицированных электронных подписей уполномоченного лица Удостоверяющего центра МЧС России в изготовленных им Сертификатах;

для хранения личного закрытого ключа использовать сертифицированный USB-ключ eToken, поддерживаемый используемым сертифицированным в соответствии с Правилами сертификации Российской

Федерации (далее – правила сертификации) средством криптографической защиты информации;

воспользоваться предоставляемыми системой услуг, пользователем которой он является, программными средствами для передачи по линиям связи в Удостоверяющий центр МЧС России запроса на выпуск Сертификата в электронном виде;

обратиться в систему услуг, пользователем которой он является, для формирования квалифицированного сертификата с областями действия отличными от областей действия действующего квалифицированного сертификата пользователя;

воспользоваться предоставляемыми системой услуг, пользователем которой он является, программными средствами, для получения и установления на своем рабочем месте изготовленный Удостоверяющим центром МЧС России Сертификат в электронном виде;

обратиться в систему услуг, пользователем которой он является, для аннулирования (отзыва) Сертификата в течение срока действия соответствующего закрытого ключа;

обратиться в систему услуг, пользователем которой он является, для приостановления действия Сертификата в течение срока действия соответствующего закрытого ключа;

обратиться в систему услуг, пользователем которой он является, для возобновления действия Сертификата в течение срока действия соответствующего закрытого ключа и срока, на который действие Сертификата было приостановлено.

2.3. Удостоверяющий центр обязан:

использовать для изготовления закрытого ключа доверенного лица Удостоверяющего центра МЧС России и формирования квалифицированной электронной подписи только прошедшие оценку соответствия в соответствии с правилами сертификации, действующими на территории Российской Федерации, средства криптографической защиты информации;

использовать закрытый ключ доверенного лица Удостоверяющего центра МЧС России только для подписи издаваемых им квалифицированных Сертификатов пользователей Удостоверяющего центра МЧС России и списков отозванных Сертификатов;

принять меры по защите закрытого ключа доверенного лица Удостоверяющего центра МЧС России от несанкционированного доступа;

организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Москвы. Синхронизировать по времени все свои программные и технические средства обеспечения деятельности;

обеспечить регистрацию пользователей Удостоверяющего центра МЧС России по заявлениям на регистрацию в соответствии с порядком регистрации, изложенным в настоящем Регламенте. Обеспечить

уникальность регистрационной информации пользователей Удостоверяющего центра МЧС России, используемой для идентификации владельцев Сертификатов;

обеспечить уникальность серийных номеров изготавливаемых Сертификатов пользователей Удостоверяющего центра МЧС России;

обеспечить уникальность значений открытых ключей в изготовленных Сертификатах пользователей Удостоверяющего центра МЧС России;

аннулировать (отозвать) Сертификат по заявлению на аннулирование (отзыв) Сертификата, поступающему от системы услуг и не позднее 3-х рабочих дней, следующих за рабочим днем в течение которого было подано заявление, занести сведения об аннулированном (отозванном) Сертификате в список отозванных Сертификатов с указанием даты и времени занесения и причины отзыва;

приостановить действие Сертификата по заявлению на приостановление действия Сертификата, поступающему от системы услуг и не позднее 3-х рабочих дней, следующих за рабочим днем в течение которого было подано заявление занести сведения о приостановленном Сертификате в список отозванных Сертификатов с указанием даты и времени занесения и признака приостановления;

возобновить действие Сертификата по заявлению на возобновление действия Сертификата (в случае поступления заявления в период срока, на который действие сертификата было приостановлено), поступающему от системы услуг и не позднее 3-х рабочих дней, следующих за рабочим днем в течение которого было подано заявление исключить сведения о сертификате, действие которого было приостановлено, из списка отозванных сертификатов;

аннулировать (отозвать) Сертификат в случае, если истек установленный срок, на который действие данного Сертификата было приостановлено;

вести реестр Удостоверяющего центра МЧС России.

В случае изготовления Удостоверяющим центром МЧС России закрытого и открытого ключа пользователя Удостоверяющий центр МЧС России обязан:

выполнять процедуру генерации ключей и их запись на сертифицированный USB-ключ eToken только с использованием сертифицированного в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации;

обеспечить сохранение в тайне изготовленного закрытого ключа пользователя;

2.4. Пользователь Удостоверяющего центра МЧС России обязан:

хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования;

не применять личный закрытый ключ, если пользователю стало известно, что этот ключ используется или использовался ранее другими лицами;

применять личный закрытый ключ только в соответствии с областями действия, указанными в соответствующем данному закрытому ключу сертификате открытого ключа;

немедленно обратиться в систему услуг, пользователем которой он является, с заявлением на аннулирование (отзыв) Сертификата в случае потери, раскрытия, искажения личного закрытого ключа, а также в случае если пользователю стало известно, что этот ключ используется или использовался ранее другими лицами;

не использовать личный закрытый ключ, связанный с Сертификатом, заявление на аннулирование (отзыв) которого подано в систему услуг, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) Сертификата систему услуг по момент времени официального уведомления пользователя об аннулировании (отзыве) Сертификата;

не использовать личный закрытый ключ, связанный с Сертификатом, заявление на приостановление действия которого подано в систему услуг, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в систему услуг по момент времени официального уведомления пользователя о приостановлении действия сертификата;

не использовать личный закрытый ключ, связанный с сертификатом открытого ключа, который аннулирован (отозван) или действие его приостановлено.

3. Порядок работы Удостоверяющего центра МЧС России

3.1. Регистрация пользователей

Порядок регистрации пользователей системы услуг в Удостоверяющем центре МЧС России изложен в Положении по предоставлению государственных и муниципальных услуг Удостоверяющим центром МЧС России, который описывает процедуры регистрации пользователей, генерации ключей, управления Сертификатами применительно к этим системам услуг.

Временем подписания электронного документа, на основании которого была проведена регистрация пользователя, считается время внесения документа в реестр Удостоверяющего центра МЧС России.

3.2. Генерация ключей

Порядок генерации закрытых ключей пользователей Удостоверяющего центра МЧС России в системах услуг изложен в Положении по предоставлению государственных и муниципальных услуг Удостоверяющим центром МЧС России, который описывает процедуры регистрации пользователей, генерации ключей, управления Сертификатами применительно к этим системам услуг.

3.3. Изготовление и получение Сертификата

Порядок изготовления и получения Сертификатов пользователей Удостоверяющего центра МЧС России в системах услуг изложен в Положении по предоставлению государственных и муниципальных услуг Удостоверяющим центром МЧС России, который описывает процедуры регистрации пользователей, генерации ключей, управления Сертификатами применительно к этим системам услуг.

Временем подписания электронного документа, на основании которого было проведено изготовление Сертификата, считается время внесения документа в реестр Удостоверяющего Центра МЧС России.

3.4. Аннулирование (отзыв) Сертификата

Для осуществления аннулирования (отзыва) Сертификата пользователь подает заявление на аннулирование (отзыв) Сертификата в систему услуг.

Аннулирование (отзыв) Сертификата пользователя Удостоверяющего центра МЧС России осуществляется Удостоверяющим центром МЧС России на основании заявления, поступающего из системы услуг в бумажной или в электронной форме.

Заявление на аннулирование (отзыв) Сертификата в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на отзыв Сертификата, а квалифицированная электронная подпись осуществляется на действующем закрытом ключе пользователя.

Заявление на аннулирование (отзыв) Сертификата формируется и подается в электронном виде в систему услуг с использованием программного обеспечения пользователя системы услуг. Система услуг установленным порядком передает заявление на аннулирование (отзыв) Сертификата, полученное от пользователя, в Удостоверяющий центр МЧС России.

Порядок формирования и передачи заявления на аннулирование (отзыв) Сертификата в электронном виде в конкретной системе услуг приводится в Положении по предоставлению государственных и муниципальных услуг Удостоверяющим центром МЧС России, описывающий процедуры управления Сертификатами в этой системе услуг.

Подача заявления на аннулирование (отзыв) Сертификата, оформленного в бумажном виде, в Удостоверяющий центр МЧС России и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на аннулирование (отзыв) Сертификата и оповещение пользователя об аннулировании (отзыве) Сертификата должны быть осуществлены не позднее 3-х рабочих дней, следующих за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

Временем аннулирования (отзыва) Сертификата признается время официального уведомления пользователя об аннулировании (отзыве) данного Сертификата.

Временем подписания электронного документа, на основании которого было проведено аннулирование (отзыв) Сертификата пользователя, считается время внесения документа в реестр Удостоверяющего Центра МЧС России.

3.5. Приостановление/возобновление действия Сертификата

Приостановление действия Сертификата

Для осуществления приостановления действия Сертификата пользователь подает заявление на приостановление действия Сертификата в систему услуг.

Приостановление действия Сертификата пользователя осуществляется Удостоверяющим центром МЧС России на основании заявления, поступающего установленным порядком из системы услуг в бумажной или электронной форме.

Заявление на приостановление действия Сертификата формируется и подается в электронном виде в систему услуг с использованием программного обеспечения пользователя системы услуг. Система услуг установленным порядком передает заявление на приостановление действия Сертификата, полученное от пользователя, в Удостоверяющий центр МЧС России.

Порядок формирования и передачи заявления на приостановление действия Сертификата в электронном виде в конкретных системах услуг приводится в Положении по предоставлению государственных и муниципальных услуг Удостоверяющим центром МЧС России, описывающий процедуры управления Сертификатами в этой системе услуг.

Действие Сертификата приостанавливается на исчисляемый в календарных днях срок. Минимальный срок приостановления действия Сертификата составляет 30 дней.

Подача заявления на приостановление действия Сертификата, оформленного в бумажном виде, в Удостоверяющий центр МЧС России и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на приостановление действия Сертификата и оповещение пользователя о приостановлении действия сертификата должны быть осуществлены не позднее 3-х рабочих дней, следующих за рабочим

днем, в течение которого было подано заявление в Удостоверяющий центр МЧС России.

Временем приостановления действия Сертификата открытого ключа признается время официального уведомления пользователя о приостановлении действия данного Сертификата.

Временем подписания электронного документа, на основании которого было проведено приостановление действия Сертификата пользователя, считается время внесения документа в реестр Удостоверяющего центра МЧС России.

В случае если в течение срока приостановления действия Сертификата пользователя в Удостоверяющий центр МЧС России не поступает заявление от системы услуг о возобновлении действия Сертификата, Сертификат аннулируется (отзывается) Удостоверяющим центром МЧС России.

Возобновление действия сертификата открытого ключа

Для осуществления возобновления действия Сертификата пользователь подает заявление на возобновление действия Сертификата в систему услуг.

Возобновление действия Сертификата пользователя осуществляется Удостоверяющим центром на основании заявления, поступающего установленным порядком из системы услуг в бумажной или электронной форме.

Заявление на возобновление действия Сертификата формируется и подается в электронном виде в систему услуг с использованием программного обеспечения пользователя системы услуг. Система услуг установленным порядком передает заявление на возобновление действия Сертификата, полученное от пользователя, в Удостоверяющий центр МЧС России.

Порядок формирования и передачи заявления на возобновление действия Сертификата в электронном виде в конкретных системах услуг, взаимодействующих с Удостоверяющим центром МЧС России, приводится в Положении по предоставлению государственных и муниципальных услуг Удостоверяющим центром МЧС России, описывающих процедуры управления Сертификатами в этой системе услуг.

Подача заявления на возобновление действия Сертификата в Удостоверяющий центр МЧС России и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на возобновление действия Сертификата и оповещение пользователя о возобновлении действия Сертификата должны быть осуществлены не позднее 3-х рабочих дней, следующих за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр МЧС России.

Временем возобновления действия Сертификата признается время официального уведомления пользователя о возобновлении действия данного Сертификата.

Временем подписания электронного документа, на основании которого было проведено возобновление действия Сертификата пользователя, считается время внесения документа в реестр Удостоверяющего Центра МЧС России.

Возобновление действия Сертификата возможно только в течение срока, на который было приостановлено действие Сертификата.

3.6. Подтверждение подлинности ЭП в электронных документах

Для подтверждения подлинности ЭП в электронных документах, циркулирующих в системах услуг, пользователь Удостоверяющего центра МЧС России подает заявление на подтверждение подлинности ЭП в электронном документе в систему услуг.

Подтверждение подлинности ЭП электронного документа осуществляет Удостоверяющий центр МЧС России на основании заявления, поступающего установленным порядком из системы услуг в бумажной форме.

Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является сменный магнитный носитель.

Электронная подпись в предоставленном электронном документе будет считаться равнозначной собственноручной подписи при выполнении следующих условий:

сертификат подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, не утратил силу (действует) на момент формирования ЭП в электронном документе - дата и время формирования ЭП в электронном документе, указанная в заявлении на подтверждение подлинности ЭП;

электронная подпись, проверенная на Сертификате с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, верна;

электронная подпись используется в соответствии со сведениями, указанными в Сертификате – в поле Extended Key Usage;

формирование электронной подписи осуществлено без нарушений условий настоящего Регламента.

Срок проведения работ по подтверждению подлинности ЭП в электронном документе и предоставлению заключения о произведенной проверке системы услуг составляет 5 рабочих дней с момента его поступления в Удостоверяющий центр МЧС России.

Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, состоящая не менее чем из 3-х человек, сформированная из числа сотрудников Удостоверяющего центра МЧС России и сопутствующих подразделений.

Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение Удостоверяющего центра МЧС

России в письменной форме, подписанное всеми членами комиссии и заверенное печатью Национального центра МЧС России.

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручными подписями всех членов комиссии.

3.7. Подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра МЧС России в изданных Сертификатах

Для подтверждения подлинности ЭП уполномоченного лица Удостоверяющего центра МЧС России в Сертификате пользователь подает заявление на подтверждение подлинности ЭП уполномоченного лица Удостоверяющего МЧС России центра в Сертификате в систему услуг.

Подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра МЧС России в Сертификате осуществляет Удостоверяющий центр МЧС России на основании заявления, поступающего установленным порядком из системы услуг в бумажной форме.

Обязательным приложением к заявлению на подтверждение подлинности ЭП уполномоченного лица в Сертификате является сменный магнитный носитель, содержащий файл Сертификата, подвергающегося процедуре проверки.

Срок проведения работ по подтверждению подлинности ЭП в электронном документе и предоставлению заключения о произведенной проверке системы услуг составляет 5 рабочих дней с момента его поступления в Удостоверяющий центр.

Проведение работ по подтверждению подлинности ЭП уполномоченного лица Удостоверяющего центра МЧС России в Сертификате осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра МЧС России и сопутствующих подразделений.

Результатом проведения работ по подтверждению подлинности ЭП уполномоченного лица Удостоверяющего центра МЧС России в Сертификате является заключение Удостоверяющего центра МЧС России в письменной форме, подписанное всеми членами комиссии и заверенное печатью Национального центра МЧС России.

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручными подписями всех членов комиссии.

4. Прочие условия

4.1. Конфиденциальность

Закрытый ключ, соответствующий Сертификату пользователя Удостоверяющего Центра МЧС России является конфиденциальной информацией данного пользователя Удостоверяющего Центра МЧС России. Удостоверяющий Центр МЧС России не осуществляет хранение закрытых ключей пользователей.

Информация о пользователях Удостоверяющего центра МЧС России, хранящаяся в Удостоверяющем центре и не подлежащая непосредственной рассылке в качестве части Сертификата считается конфиденциальной.

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

Открытая информация может публиковаться по решению Удостоверяющего Центра МЧС России. Место, способ и время публикации открытой информации определяется Удостоверяющим Центром МЧС России.

Информация, включаемая в Сертификатов пользователей Удостоверяющего центра МЧС России и списки отозванных Сертификатов, издаваемые Удостоверяющим Центром МЧС России, не считается конфиденциальной.

Удостоверяющий Центр МЧС России имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях установленных законодательством Российской Федерации.

4.2. Плановая смена ключей уполномоченного лица Удостоверяющего центра МЧС России

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) уполномоченного лица Удостоверяющего центра МЧС России выполняется не ранее, чем через 3 года 10 месяцев и не позднее, чем через 4 года после начала действия закрытого ключа уполномоченного лица Удостоверяющего центра МЧС России.

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

уполномоченное лицо Удостоверяющего центра МЧС России формирует новый закрытый и соответствующий ему открытый ключ;

уполномоченное лицо Удостоверяющего центра МЧС России изготавливает новый Сертификат, соответствующий новому закрытому ключу, и подписывает его электронной подписью с использованием нового закрытого ключа.

Старый закрытый ключ доверенного лица Удостоверяющего центра МЧС России используется в течение своего срока действия для формирования списков отозванных Сертификатов в электронной форме, изданных Удостоверяющим центром в период действия старого закрытого ключа уполномоченного лица Удостоверяющего центра МЧС России.

4.3. Компрометация ключа доверенного лица Удостоверяющего центра МЧС России

В случае компрометации или угрозы компрометации закрытого ключа доверенного лица Удостоверяющего центра МЧС России выполняется

внеплановая смена ключей уполномоченного лица Удостоверяющего центра МЧС России.

Процедура внеплановой смены ключей доверенного лица Удостоверяющего центра МЧС России выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица Удостоверяющего центра МЧС России.

В случае компрометации ключа доверенного лица Удостоверяющего центра МЧС России после выполнения процедуры внеплановой смены ключей, Сертификат доверенного лица Удостоверяющего центра МЧС России аннулируется (отзывается) путем занесения в список отозванных Сертификатов.

По факту компрометации закрытого ключа доверенного лица Удостоверяющего центра МЧС России в МЧС России проводится служебное расследование, результаты которого должны быть отражены в соответствующем акте.

4.4. Компрометация ключа пользователя Удостоверяющего центра МЧС России

Пользователь Удостоверяющего центра МЧС России самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа.

В случае компрометации или угрозы компрометации закрытого ключа пользователь подает в систему услуг заявление на отзыв Сертификата в соответствии с правилами, установленными в системе услуг.

4.5. Прекращение деятельности Удостоверяющего центра МЧС России

Прекращение деятельности Удостоверяющего центра МЧС России может быть осуществлено на основании приказа МЧС России, решения начальника Национального центра МЧС России и в порядке, установленном внутренними документами МЧС России.

Все Сертификаты пользователей, выданные Удостоверяющим центром МЧС России аннулируются.

4.6. Опубликование и оповещение

Удостоверяющий центр МЧС России обязан официально уведомить о факте аннулирования (отзыва) Сертификата его владельца.

Срок уведомления – не позднее 3-х рабочих дней, следующих за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр МЧС России от системы услуг на аннулирование (отзыв) Сертификата.

Официальным уведомлением о факте аннулирования (отзыва) Сертификата является опубликование списка отозванных Сертификатов, содержащего сведения об аннулированном (отозванном) Сертификате.

Временем опубликования считается время издания списка отозванных Сертификатов, указанное в поле thisUpdate изданного списка отозванных Сертификатов.

Информация о размещении списка отозванных Сертификатов заносится в Сертификат пользователя Удостоверяющего центра МЧС России в поле CRL Distribution Point.

Удостоверяющий Центр МЧС России обязан официально уведомить о факте приостановления действия Сертификата его владельца.

Срок уведомления – не позднее 3-х рабочих дней, следующих за рабочим днем в течение которого было подано заявление в Удостоверяющий центр МЧС России от системы услуг на приостановление действия Сертификата.

Официальным уведомлением о факте приостановления действия Сертификата является опубликование списка отозванных Сертификатов, содержащего сведения о Сертификате, действие которого было приостановлено. Временем опубликования считается время издания списка отозванных Сертификатов, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных Сертификатов заносится в Сертификат пользователя Удостоверяющего центра МЧС России в поле CRL Distribution Point.

Удостоверяющий центр МЧС России обязан официально уведомить о факте возобновления действия Сертификата его владельца.

Срок уведомления – не позднее 3-х рабочих дней, следующих за рабочим днем в течение которого было подано заявление в Удостоверяющий центр МЧС России от системы услуг на возобновление действия Сертификата.

Официальным уведомлением о факте возобновления действия Сертификата является опубликование списка отозванных Сертификатов, не содержащего сведений о Сертификате, действие которого было возобновлено. Временем опубликования считается время издания списка отозванных Сертификатов, указанное в поле thisUpdate изданного списка отозванных Сертификатов.

Информация о размещении списка отозванных Сертификатов заносится в Сертификат пользователя Удостоверяющего центра МЧС России в поле CRL Distribution Point.

4.7. Сроки действия ключей уполномоченного лица Удостоверяющего центра МЧС России

Срок действия закрытого ключа доверенного лица Удостоверяющего центра МЧС России составляет 5 лет.

Начало периода действия закрытого ключа доверенного лица Удостоверяющего центра МЧС России исчисляется с даты и времени его генерации.

Срок действия Сертификата, соответствующего закрытому ключу доверенного лица Удостоверяющего центра МЧС России составляет 5 лет.

4.8. Сроки действия ключей пользователей

Установленные сроки действия закрытых ключей и Сертификатов в конкретной системе услуг МЧС России приведены в Положении по предоставлению государственных и муниципальных услуг Удостоверяющим центром МЧС России, описывающему процедуры управления сертификатами в этой системе услуг.

Начало периода действия закрытого ключа пользователя исчисляется с даты и времени начала действия соответствующего Сертификата.

4.9. Хранение Сертификатов в Удостоверяющем центре МЧС России

Срок хранения Сертификата в Удостоверяющем центре МЧС России осуществляется в течение всего периода его действия и 5 лет после его аннулирования (отзыва).

По истечении указанного срока хранения Сертификаты переводятся в режим архивного хранения.

Срок хранения архивных документов - 5 лет.

Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией, формируемой из числа сотрудников Национального центра МЧС России.

4.10. Обработка персональных данных пользователей Удостоверяющего центра

С целью предоставления услуг Удостоверяющий центр МЧС России осуществляет сбор, обработку и хранение персональных данных в объеме, необходимом для выдачи Сертификата.

Удостоверяющий центр МЧС России обеспечивает защиту персональных данных в соответствии с требованиями законодательства Российской Федерации.

4.11. Структура сертификатов открытого ключа и списков отозванных сертификатов

Удостоверяющий центр МЧС России издает Сертификаты пользователей в электронной форме формата X.509 версии 3 и список отозванных сертификатов (СОС) в электронной форме формата X.509 версии 2.

5. Обеспечение безопасности информационных ресурсов

Для обеспечения надлежащей работы Удостоверяющего центра МЧС России ответственное подразделение Национального центра МЧС России выполняет организационные и технические меры, направленные на защиту обрабатываемой информации ограниченного доступа.

Для взаимодействия с ресурсами Удостоверяющего центра МЧС России назначаются приказом доверенное лицо Удостоверяющего центра МЧС России, а также операторы Удостоверяющего центра МЧС России.

Доступ к ресурсам Удостоверяющего центра МЧС России предоставляется исключительно уполномоченным сотрудникам с правами, ограничивающими их должностными обязанностями.

Для защиты ресурсов Удостоверяющего центра МЧС России и информации ограниченного доступа применяются технические меры защиты в соответствии с требованиями законодательства Российской Федерации.

Для технической защиты ресурсов Удостоверяющего центра МЧС России применяются исключительно средства защиты, прошедшие сертификацию ФСТЭК России.

Средства защиты информационных ресурсов Удостоверяющего центра МЧС России эксплуатируются в соответствии с правилами эксплуатации и рекомендациями производителей указанных средств.

Администраторы и пользователи средств защиты информации в своей работе также руководствуются утвержденными инструкциями по работе со средствами защиты информации.

Для обеспечения целостности и доступности реестров сертификатов, выпущенных Удостоверяющим центром МЧС России уполномоченным подразделением, ответственным за эксплуатацию удостоверяющего центра, регулярно осуществляется резервное копирование реестра Сертификатов, а также баз данных Центра Сертификации и Центра Регистрации Удостоверяющего центра МЧС России. Резервное копирование производится согласно положениям «Описания технологического процесса обработки информации».

В своей работе ответственные сотрудники Удостоверяющего центра МЧС России руководствуются положениями настоящего Регламента, действующими должностными инструкциями, а также иными внутренними документами МЧС России и нормами законодательства Российской Федерации.

6. Разрешение споров

Сторонами в споре, в случае его возникновения, считаются Национальный центр МЧС России, являющийся подразделением выполняющим функции Удостоверяющего центра МЧС России, и пользователь Удостоверяющего центра МЧС России.

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

Для юридических лиц и ПБОЮЛ:

При отсутствии согласия спор между Сторонами подлежит рассмотрению в Арбитражном суде города Москвы.

Для физических лиц, в том числе занимающихся частной практикой:

При отсутствии согласия спор между Сторонами подлежит рассмотрению в районном суде города Москвы.

В случае если в соответствии с гражданским процессуальным законодательством РФ спор по настоящему Регламенту подсуден мировому судье, то он подлежит рассмотрению мировым судьей по месту нахождения Национального центра МЧС России.

7. Ответственность сторон

Размер ответственности Национального центра МЧС России и присоединившейся стороны при нарушении условий настоящего Регламента определяется в соответствии с договором на обслуживание в системе услуг, подписанным присоединившейся стороной.

8. Реквизиты

Национальный центр МЧС России, Удостоверяющий Центр
Адрес: 121357, г. Москва, ул. Ватутина, д.1
Адрес электронной почты: UC.FGBU.NCUKS@yandex.ru

Приложение к Регламенту
Удостоверяющего центра электронной подписи
Министерства Российской Федерации
по делам гражданской обороны,
чрезвычайным ситуациям и
ликвидации последствий стихийных бедствий

Термины и определения

Аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона № 63-ФЗ «Об электронной подписи»;

Система услуг - обобщенное понятие информационной системы, эксплуатирующейся в рамках системы межведомственного электронного взаимодействия или в составе корпоративной информационной системы МЧС России, в которой используются закрытые ключи и Сертификаты, и предоставляющей определенные услуги пользователям - участникам этой системы.

Владелец сертификата ключа проверки электронной подписи (далее – владелец Сертификата)– лицо, на имя которого Удостоверяющим центром выдан сертификат проверки электронной подписи и которое владеет соответствующим закрытым ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

Государственная услуга, предоставляемая федеральным органом исполнительной власти, органом государственного внебюджетного фонда, исполнительным органом государственной власти субъекта Российской Федерации, а также органом местного самоуправления при осуществлении отдельных государственных полномочий, переданных федеральными законами и законами субъектов Российской Федерации (далее - государственная услуга), - деятельность по реализации функций соответственно федерального органа исполнительной власти, государственного внебюджетного фонда, исполнительного органа государственной власти субъекта Российской Федерации, а также органа местного самоуправления при осуществлении отдельных государственных полномочий, переданных федеральными законами и законами субъектов Российской Федерации (далее - органы, предоставляющие государственные услуги), которая осуществляется по запросам заявителей в пределах установленных нормативными правовыми актами Российской Федерации и нормативными правовыми актами субъектов Российской Федерации полномочий органов, предоставляющих государственные услуги

Договор на обслуживание в системе услуг (договор на обслуживание) – договор, заключенный между физическим лицом, в том числе ПБОЮЛ и физическим лицом, занимающимся частной практикой, или юридическим лицом на пользование услугами (обслуживание) в системе услуг.

Единый государственный реестр Удостоверяющих Центров

Закрытый ключ электронной подписи - уникальная последовательность символов, известная владельцу сертификата проверки электронной подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.

Закрытый ключ электронной подписи действует на определенный момент времени (действующий закрытый ключ) если:

наступил момент времени начала действия закрытого ключа;

срок действия закрытого ключа не истек;

сертификат проверки электронной подписи, соответствующий данному закрытому ключу не аннулирован (отозван) и действие его не приостановлено.

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.

Ключ электронной подписи (далее – закрытый ключ)- уникальная последовательность символов, предназначенная для создания электронной подписи;

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

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган); в рамках работы Удостоверяющего Центра Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее – Удостоверяющий центр МЧС России) все выпускаемые сертификаты являются квалифицированными;

Компрометация ключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Корпоративная информационная система - информационная система в МЧС России, объединяющая в себе различные информационные системы внутри Министерства.

Межведомственное информационное взаимодействие - осуществляемое в целях предоставления государственных и муниципальных услуг взаимодействие по вопросам обмена документами и информацией, в том числе в электронной форме, между органами, предоставляющими государственные услуги, органами, предоставляющими муниципальные услуги, подведомственными государственным органам или органам местного самоуправления организациями, государственных или муниципальных услуг, иными государственными органами, органами местного самоуправления, многофункциональными центрами.

Область действия сертификата ключа проверки электронной подписи – включенные в сертификат открытого ключа подписи сведения об отношениях, при которых электронный документ с электронной цифровой подписью, соответствующей сертифицированному открытому ключу подписи, будет иметь юридическое значение.

Обработка заявления на аннулирование (отзыв), приостановление/возобновление действия сертификата – совокупность действий по занесению сведений об аннулировании (отзыве), приостановлении/возобновлении действия сертификата в реестр Удостоверяющего центра и уведомлению пользователя об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата.

Открытый ключ электронной цифровой подписи (открытый ключ) - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Пользователь системы услуг – физическое или юридическое лицо, заключившее договор на обслуживание в системе услуг.

Пользователь Удостоверяющего центра – физическое лицо или, выступающее в лице своего уполномоченного представителя, юридическое лицо, внесенное в реестр Удостоверяющего центра.

Портал государственных и муниципальных услуг - государственная информационная система, обеспечивающая предоставление государственных и муниципальных услуг в электронной форме, а также доступ заявителей к сведениям о государственных и муниципальных услугах, предназначенным для распространения с использованием информационно-телекоммуникационной сети Интернет и размещенным в государственных и муниципальных информационных системах, обеспечивающих ведение реестров государственных и муниципальных услуг.

Предоставление государственных и муниципальных услуг в электронной форме - предоставление государственных и муниципальных услуг с использованием информационно-телекоммуникационных технологий, в том числе с использованием портала государственных и муниципальных услуг, многофункциональных центров, универсальной электронной карты и других средств, включая осуществление в рамках такого предоставления электронного взаимодействия между государственными органами, органами местного самоуправления, организациями и заявителями;

Псевдоним – вымышленное имя физического лица, которое это лицо сознательно и легально принимает для регистрации в Удостоверяющем центре.

Рабочий день Удостоверяющего центра МЧС России (далее – рабочий день) – промежуток времени с 10:00 по 17:00 каждого дня недели за исключением выходных и праздничных дней.

Рассмотрение заявления на аннулирование (отзыв), приостановление/возобновление действия сертификата, – принятие уполномоченным лицом Удостоверяющего центра решения об обработке заявления на основе предоставленных системой услуг документов.

Реестр Удостоверяющего центра – набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

реестр заявлений на регистрацию пользователя в Удостоверяющем центре;

реестр зарегистрированных пользователей Удостоверяющего центра;

реестр запросов на сертификат открытого ключа подписи;

реестр заявлений на аннулирование (отзыв) сертификата открытого ключа подписи;

реестр заявлений на приостановление/возобновление действия сертификата открытого ключа подписи;

реестр сертификатов открытых ключей подписи;

реестр изготовленных списков отозванных сертификатов;

служебные документы Удостоверяющего центра.

Российское пространство телекоммуникационных объектных идентификаторов – диапазон объектных идентификаторов, выделенный ассоциацией IANA для идентификации телекоммуникационных объектов Российской Федерации.

Сертификат ключа проверки электронной подписи (Сертификат) - электронный документ или документ на бумажном носителе, структура которого определяется настоящим Регламентом и который выдается Удостоверяющим центром пользователю системы услуг и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Система межведомственного электронного взаимодействия (СМЭВ) - федеральная государственная информационная система, включающая информационные базы данных, в том числе содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа через систему взаимодействия к их информационным системам, сведения об истории движения в системе взаимодействия электронных сообщений при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в электронной форме, а также программные и технические средства, обеспечивающие взаимодействие информационных систем органов и организаций, используемых при предоставлении в электронной форме государственных и муниципальных услуг и исполнении государственных и муниципальных функций.

Список отозванных сертификатов (СОС) – электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

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

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

Удостоверяющий центр Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (далее - Удостоверяющий центр МЧС России) - функциональное подразделение Национального центра управления в кризисных ситуациях Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, выполняющее следующие основные функции:

создает и выдает сертификаты ключей проверки электронных подписей;

создает ключи электронных подписей с гарантией сохранения в тайне закрытого ключа электронной подписи;

приостанавливает и возобновляет действие сертификатов ключей проверки электронных подписей, а также аннулирует их;

ведет реестр Удостоверяющего центра, обеспечивает его актуальность;

проверяет уникальность открытых ключей;

выдает сертификаты ключей проверки электронных подписей с информацией об их действии;

осуществляет подтверждение подлинности электронной подписи в электронном документе.

Удостоверяющий центр использует для изготовления закрытых ключей и сертификатов ключей проверки электронных подписей средство криптографической защиты информации компании «КРИПТО-ПРО» «КриптоПро CSP».

Уполномоченный представитель юридического лица – физическое лицо, наделенное юридическим лицом полномочиями на получение и пользование услугами Удостоверяющего центра.

Установленный порядок – порядок взаимодействия системы услуг с клиентами и структурными подразделениями, определенный действующими регламентными документами.

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

Электронный документ – документ, информация в котором представлена в электронно-цифровой форме.

Электронная подпись (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, а также контроля отсутствия искажения информации в электронном документе;

Электронное правительство -

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий центр и системы услуг МЧС России осуществляют свою работу в соответствии со следующими стандартами PKCS:

PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. _____ использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные. Электронный документ, оформленный с соблюдением требований PKCS#7 Signed, является электронным документом, содержащим электронную цифровую подпись;

PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа подписи. Электронный документ, оформленный с соблюдением требований PKCS#10, содержит информацию о сертифицируемом открытом ключе, используемом криптографическом средстве и данные, необходимые для идентификации владельца сертифицируемого открытого ключа электронной цифровой подписи.

Internet Assigned Numbers Authority (IANA, ассоциация IANA) – международная организация, координирующая выделение объектных идентификаторов, предназначенных для идентификации телекоммуникационных объектов.