«Утвержден»

Генеральным директором

ЗАО «МО ПНИЭИ»

Монастырецким В. И.

05 июля 2012 г.

РЕГЛАМЕНТ

Аккредитованного удостоверяющего центра ЗАО «МО ПНИЭИ».

Редакция № 1

Москва. 2012

СОДЕРЖАНИЕ.

1. Сведения об Удостоверяющем центре

«Удостоверяющий центр ЗАО «МО ПНИЭИ», является структурным подразделением ЗАО «МО ПНИЭИ».

Удостоверяющий центр в качестве профессионального участника рынка услуг по изготовлению и выдаче сертификатов ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации в соответствии с Уставом и лицензиями:

1.ЛИЦЕНЗИЯ ЛЗ №0018362
Регистрационный № 8022 П от 26 ноября 2009 г.
Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем

2.ЛИЦЕНЗИЯ ЛЗ №0018363
Регистрационный № 8023 Х от 26 ноября 2009 г.
Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление технического обслуживания шифровальных (криптографических) средств

3.ЛИЦЕНЗИЯ ЛЗ №0018364
Регистрационный № 8024 Р от 26 ноября 2009 г.
Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление распространения шифровальных (криптографических) средств

4.ЛИЦЕНЗИЯ ЛЗ 0018365
Регистрационный № 8025 У.от 26 ноября 2009 г.
Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление предоставления услуг в области шифрования информации.

5. ЛИЦЕНЗИЯ ЛЗ №0018366
Регистрационный № 8026 К.от 26 ноября 2009 г.
Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление разработки и (или) производства средств защиты конфиденциальной информации.

6.ЛИЦЕНЗИЯ ГТ №0044154
Регистрационный № 10178 С от 22 февраля 2011 г.
Центр по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну

7.ЛИЦЕНЗИЯ ГТ №0044155
Регистрационный № 10179 М от 22 февраля 2011 г.
Центр по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны

8. ЛИЦЕНЗИЯ №002143
Регистрационный № 0766 от11 декабря 2008 г.
Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации.

9.ЛИЦЕНЗИЯ №002144
Регистрационный № 0459 от11 декабря 2008 г.
Федеральной службы по техническому и экспортному контролю на осуществление разработки и (или) производства средств защиты конфиденциальной информации.

2. Термины и определения.

Электронный документ - документ, в котором информация представлена в электронной 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.
Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
Квалифицированный сертификат ключа проверки электронной подписи - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.
Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.
Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;
Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).
Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей.
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.
Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.
Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, содержащий информацию из сертификата ключа проверки электронной подписи и заверенный собственноручной подписью администратора (уполномоченного лица)Удостоверяющего центра и печатью ЗАО «МО ПНИЭИ».
Список аннулированных сертификатов (САС) – электронный документ с электронной подписью Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей подписи, которые на определенный момент времени были отозваны.
Обработка заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи– совокупность действий по занесению сведений об аннулировании (отзыве) сертификата ключа подписи в реестр Удостоверяющего центра и уведомлению пользователя об аннулировании (отзыве) сертификата ключа подписи.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 9 часов 00 минут до 18 часов по московскому времени каждого дня недели за исключением субботы, воскресенья и праздничных нерабочих дней.

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

Корпоративная информационная система (корпоративная ИС) - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

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

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

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр и Участники настоящего Регламента используют описанные в PKCS#7 типы PKCS#7 Signed – подписанные данные, PKCS#7 Enveloped – зашифрованные, PKCS#7 Signed And Enveloped – подписанные и зашифрованные данные;
- PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи .

3. Общие положения.

3.1. Статус Регламента.

3.1.1 Регламент Удостоверяющего центра, именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

3.1.2 Регламент устанавливает общий порядок и условия предоставления Удостоверяющим центром Пользователю корпоративной ИС, а так же ИС общего пользования, присоединившемуся к Регламенту в порядке, предусмотренном статьёй 428 ГК РФ, услуг по изготовлению и выдаче сертификатов ключей проверки электронной подписи и дополнительных услуг, связанных с управлением сертификатами ключей проверки электронной подписи включая обязанности пользователей, и членов группы администрирования УЦ, режимы работы, принятые форматы данных и мероприятия, необходимые для безопасной работы удостоверяющего центра.

3.1.3 Любое заинтересованное лицо может ознакомиться с Регламентом на сайте ЗАО «МО ПНИЭИ» по адресу: http://www.security.ru/ca/mo_acc_regl.pdf , либо в офисе Удостоверяющего центра по адресу г. Москва, ул. Сущевский Вал, дом 16, строенте5, 2-й этаж, и по запросу получить его копию за плату, не превышающую расходов на ее изготовление.

3.1.4 Присоединение к Регламенту пользователя корпоративной ИС, а так же ИС общего пользования производится путем подписания и предоставления в Удостоверяющий центр «Заявления о регистрации в реестре Пользователей Удостоверяющего центра ЗАО «МО ПНИЭИ» и изготовлению сертификата ключа проверки электронной подписи» по форме Приложений № 1, 2.

3.1.5 После присоединения в установленном порядке Пользователя корпоративной ИС, а так же ИС общего пользования к Регламенту, Стороны вступают в соответствующие договорные отношения на неопределённый срок.

3.1.6 Пользователь корпоративной ИС, а так же ИС общего пользования имеет право в одностороннем порядке без обращения в суд расторгнуть настоящий Регламент, письменно уведомив об этом ЗАО «МО ПНИЭИ» за один месяц до дня расторжения. Уведомление о расторжении, полученное ЗАО «МО ПНИЭИ» от Пользователя корпоративной ИС, а так же ИС общего пользования, является основанием для обязательного аннулирования сертификатов ключей подписей Пользователей УЦ, уполномоченных данным Пользователем корпоративной ИС, а так же ИС общего пользования. Датой аннулирования указанных сертификатов ключей Пользователей УЦ будет дата расторжения Регламента. При этом Стороны до дня прекращения действия настоящего Регламента обязаны разрешить между собой все денежные и иные имущественные вопросы, связанные с настоящим Регламентом.

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

3.1.8 Любые справки по вопросам, связанным с оказанием услуг Удостоверяющего центра, предоставляются сотрудниками Удостоверяющего центра по телефону (495) 780-48-38 (доб.103,106,107).

3.2. Применение Регламента.

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

3.2.2 В случае противоречия и/или расхождения названия какой-либо статьи со смыслом какого-либо пункта в ней содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

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

3.3. Изменения (дополнения) Регламента.

3.3.1 Внесение изменений (дополнений) в Регламент, в том числе в приложения к нему, производится только по предварительному уведомлению Пользователя корпоративной ИС, а так же ИС общего пользования.

3.3.2 Уведомление Пользователя корпоративной ИС, а так же ИС общего пользования о внесении изменений (дополнений) в Регламент осуществляется путем размещения указанных изменений (дополнений) на сайте ЗАО «МО ПНИЭИ» http://www.security.ru/ca/mo_acc_regl.pdf

3.3.3 Все изменения (дополнения), вносимые в Регламент и не связанные с изменением законодательства РФ вступают в силу и становятся обязательными для Сторон по истечении 10 (Десяти) календарных дней с даты размещения указанных изменений и дополнений в Регламенте на сайте ЗАО «МО ПНИЭИ» http://www.security.ru/ca/mo_acc_regl.pdf

3.3.4 Все изменения (дополнения), вносимые в Регламент в связи с изменением законодательной и нормативной базы, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

3.3.5 Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех Пользователей УЦ, Пользователей корпоративной ИС, а так же ИС общего пользования, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

3.4. Услуги, предоставляемые Удостоверяющим центром.

3.4.1 Внесение в реестр Удостоверяющего Центра регистрационной информации о Пользователях УЦ.

3.4.2 Изготовление сертификатов ключей проверки электронной подписи Пользователей УЦ в электронной форме.

3.4.3 Изготовление ключей электронных подписей по обращению пользователей УЦ с гарантией сохранения в тайне ключа электронной подписи пользователя

3.4.4 Изготовление копий сертификатов ключей проверки электронной подписи Пользователей УЦ на бумажном носителе.

3.4.5 Ведение реестра изготовленных сертификатов ключей электронной подписи Пользователей УЦ.

3.4.6 Предоставление копий сертификатов ключей проверки электронной подписи в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам Пользователей УЦ.

3.4.7 Аннулирование (отзыв) сертификатов ключей проверки электронной подписи по обращениям Владельцев сертификатов ключей проверки электронной подписи

3.4.8 Предоставление Пользователям УЦ сведений об аннулированных сертификатах ключей проверки электронной подписи.

3.4.9 Подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям Пользователей УЦ.

3.4.10 Подтверждение подлинности электронной подписи Удостоверяющего центра в изготовленных им сертификатах ключей проверки электронной подписи по обращениям Пользователей УЦ.

4. Права и обязанности сторон.

4.1. Удостоверяющий центр имеет право:

4.1.1 Отказать в аннулировании (отзыве) сертификата ключа проверки электронной подписи Пользователя УЦ в случае, если истек установленный срок действия ключа электронной подписи, соответствующего этому сертификату.

4.1.2 Аннулировать (отозвать) сертификат ключа проверки электронной подписи Пользователя УЦ в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного (отозванного) сертификата ключа проверки электронной подписи и указанием обоснованных причин.

4.1.3 Отказать в изготовлении сертификата ключа проверки электронной подписи Пользователя УЦ в случае, если использованное Пользователем УЦ для формирования запроса на сертификат ключа проверки электронной подписи средство криптографической защиты информации не поддерживается Удостоверяющим центром.

4.2. Пользователь УЦ имеет право:

– получить список аннулированных (отозванных) сертификатов ключей проверки электронной подписи изготовленный Удостоверяющим центром;

– применять сертификат ключа проверки электронной Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в сертификатах ключа проверки электронной подписи изготовленных Удостоверяющим центром;

– применять сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи;

– применять список отозванных сертификатов ключей проверки электронной подписи, изготовленный Удостоверяющим центром, для проверки статуса сертификатов ключей проверки электронной подписи;

– обратиться в Удостоверяющий центр за подтверждением подлинности электронных подписей в электронных документах;

– обратиться в Удостоверяющий центр за подтверждением подлинности электронных подписей Удостоверяющего центра в изготовленных им сертификатах ключей проверки электронной подписи;

– обратиться в Удостоверяющий центр для аннулирования (отзыва) сертификата ключа проверки электронной подписи, владельцем которого он является, в течение срока действия соответствующего электронной подписи.

4.3. Обязанности Удостоверяющего центра.

4.3.1 Удостоверяющий центр обязан использовать для изготовления ключа электронной подписи Удостоверяющего центра и формирования электронной подписи, только сертифицированные в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации.

4.3.2 Удостоверяющий центр обязан использовать ключ электронной подписи Удостоверяющего центра только для подписи издаваемых им сертификатов ключей проверки электронной подписи Пользователей УЦ и списков отозванных сертификатов.

4.3.3 Удостоверяющий центр обязан принять меры по защите ключа электронной подписи Удостоверяющего центра от несанкционированного доступа.

4.3.4 Удостоверяющий центр обязан организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Москвы. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

4.3.5 Удостоверяющий центр обязан обеспечить регистрацию пользователей Удостоверяющего центра по заявлениям на регистрацию в соответствии с порядком регистрации, изложенным в Регламенте.

4.3.6 Удостоверяющий центр обязан обеспечить уникальность регистрационной информации Пользователей УЦ, используемой для идентификации владельцев сертификатов ключей проверки электронной подписи.

4.3.7 В случае изготовления Удостоверяющим центром ключа электронной подписи пользователя, Удостоверяющий центр обязан:

- выполнять процедуру генерации ключей и их запись на сменный носитель только с использованием сертифицированного в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации;
- Обеспечить сохранение в тайне изготовленного ключа электронной подписи пользователя.

4.3.8 Удостоверяющий центр обязан обеспечить изготовление сертификата ключа проверки электронной подписи зарегистрированного Пользователя УЦ в соответствии с порядком, определенным в Регламенте.

Удостоверяющий центр обязан:

- Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей электронной подписи Пользователей УЦ;
- Обеспечить уникальность значений ключей проверки электронных подписей в изготовленных сертификатах ключей проверки электронной подписи Пользователей УЦ.

4.3.9 Удостоверяющий центр обязан аннулировать (отозвать) сертификат ключа проверки электронной подписи по заявлению на аннулирование (отзыв) сертификата ключа проверки электронной подписи, поступающему от его владельца и, не позднее 1 (одного) рабочего дня, следующего 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.

4.3.10 Удостоверяющий центр обязан опубликовывать актуальный Список отозванных сертификатов ключей проверки электронной подписи по адресу http:/www.security.ru/ca/mo_accredited.crl (список адресов для публикации может быть изменен и дополнен без изменения данного Регламента, при изменении и/или дополнении списка адресов для публикации сведения об этом доводятся до участников Регламента.

4.4. Обязанности Владельца сертификата ключа электронной подписи.

4.4.1 Владелец сертификата ключа проверки электронной подписи обязан хранить в тайне личный ключ электронной подписи, принимать все возможные меры

для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

4.4.2 Владелец сертификата ключа проверки электронной подписи обязан не применять личный ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

4.4.3 Владелец сертификата ключа проверки электронной подписи обязан применять личный ключ электронной подписи только в соответствии с областями действия, указанными в соответствующем данному ключу электронной подписи сертификате ключа проверки электронной подписи..

4.4.4 Владелец сертификата ключа проверки электронной подписи обязан немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) сертификата ключа проверки электронной подписи в случае потери, раскрытия, искажения личного ключа электронной подписи, а также в случае, если пользователю стало известно, что этот ключ используется или использовался ранее другими лицами.

4.4.5 Владелец сертификата ключа проверки электронной подписи обязан не использовать личный ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование (отзыв) которого подано в Удостоверяющий центр в течение времени, исчисляемого с момента времени подачи заявления на аннулирование, (отзыв) сертификата в Удостоверяющий центр по момент времени официального уведомления пользователя об аннулировании (отзыве) сертификата.

4.4.6 Владелец сертификата ключа проверки электронной подписи обязан не использовать личный ключ электронной подписи, связанный с аннулированным (отозванным) сертификатом ключа проверки электронной подписи.

5 Ответственность сторон.

5.1 Сторона, не исполнившая или ненадлежащим образом исполнившая свои обязательства по Регламенту, обязана в полном объеме возместить убытки, причиненные другой Стороне.

5.2 Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

5.3 ЗАО «МО ПНИЭИ» не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по Регламенту, а также возникшие в связи с этим убытки в случаях:

- если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлении Пользователя УЦ;
- подделки, подлога либо иного искажения уполномоченным представителем Пользователя УЦ либо третьими лицами информации, содержащейся в заявлении либо иных документах, предоставленных одной стороне от имени другой стороны.

5.4 ЗАО «МО ПНИЭИ» несет ответственность за убытки при использовании ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя УЦ, только в случае если данные убытки возникли при компрометации ключа электронной подписи Удостоверяющего Центра, либо вследствие несоответствий сведений в сертификате ключа проверки электронной подписи сведениям, указанным в Заявлении на регистрацию Пользователя УЦ.

5.5 В случае если Сторона проявит недобросовестность при исполнении своих обязательств по Регламенту, то другая сторона вправе публично известить об этом других участников корпоративной информационной системы или информационной системы общего пользования..

5.6 Выплата пени и возмещение убытков не освобождает Стороны от выполнения обязательств в натуре.

5.7 Ответственность Сторон, не урегулированная положениями Регламента, регулируется законодательством Российской Федерации.

6 Разрешение споров.

6.1 Сторонами в споре, в случае его возникновения, считаются ЗАО «МО ПНИЭИ» и Пользователь корпоративной ИС или ИС общего пользования.

6.2 Все споры и разногласия между Сторонами, возникающие из Регламента, разрешаются в Арбитражном суде города Москвы.

7 Порядок пользования услугами Удостоверяющего центра.

7.1 Для регистрации с целью получения квалифицированного сертификата Пользователь, либо лицо им уполномоченное, предоставляет в Удостоверяющий центр, в организацию - партнер ЗАО «МО ПНИЭИ» или индивидуальному предпринимателю, действующим от имени ЗАО МО ПНИЭИ на основании Договора поручения или доверенности заявление о регистрации в реестре Пользователей Удостоверяющего центра ЗАО «МО ПНИЭИ» на имя его руководителя (Приложения № 1,2).и, в случае необходимости, доверенность (на уполномоченное лицо) на осуществление процедуры регистрации для получения сертификата ключа проверки электронной подписи (Приложение №3).

В случае регистрации юридического лица, необходимо предъявить учредительные документы, документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц, и свидетельство о постановке на учет в налоговом органе заявителя либо нотариально копии указанных документов. Если физическое лицо, указываемое в сертификате юридического лица, действует от его имени на основании доверенности, указанная доверенность должна быть представлена вместе с перечисленными документами.

В случае регистрации физического лица, необходимо представить документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность, либо нотариально заверенные копии этих документов, а так же страховое свидетельство государственного пенсионного страхования или его нотариально заверенную копию.

7.2 В случае невозможности личного присутствия Пользователя, либо лица им уполномоченного, в Удостоверяющем центре, заявление о регистрации направляется в адрес Удостоверяющего центра ЗАО «МО ПНИЭИ» в виде почтового отправления с уведомлением о доставке, либо в виде сканированной копии по электронной почте, или по факсу. Нотариально заверенные копии страхового свидетельства, учредительных документов и документов, удостоверяющих личность направляются в адрес Удостоверяющего центра ЗАО «МО ПНИЭИ» в виде почтового отправления с уведомлением о доставке.

Примечание:

Допускается по согласованию с организатором корпоративной ИС или ИС общего пользования использование формы заявления о регистрации, не представленной в настоящем регламенте. В этом случае форма заявления о регистрации должна включать перечень регистрационные данные не меньший, чем в формах, приведенных в Приложениях 1,2

7.3 Администратор Центра регистрации Удостоверяющего центра или лицо, уполномоченное организацией - партнером ЗАО «МО ПНИЭИ» или индивидуальный предприниматель, действующие от имени ЗАО МО ПНИЭИ на основании Договора поручения проводят (при необходимости) мероприятия, направленные на выявление несоответствия заявленных Пользователем сведений (атрибутов). При выявлении такого несоответствия УЦ может потребовать от Пользователя его устранения или принять решение о прекращении договорных отношений с Пользователем.

7.4 ЗАО «МО ПНИЭИ» выставляет счет на оплату услуг по изготовлению сертификата ключа проверки электронной подписи (и ключа электронной подписи) Пользователя в соответствии с настоящим Регламентом.

7.5 После оплаты Пользователем выставленного счета, Администратор Центра регистрации на основании полноты и достаточности предоставленных документов производит регистрацию пользователя в Удостоверяющем Центре.

7.6 Используя ПО Центр Регистрации, администратор УЦ формирует ключ и лицензию регистрации пользователя. В лицензию регистрации пользователя заносятся дополнения, необходимые для обеспечения функционирования прикладной системы и системы управления ключами. В лицензии регистрации устанавливается дополнение **Регламент регистрации**. В лицензию регистрации записываются сертификаты ЦС, ЦР и САС ЦС и СОЛ ЦР. При формировании имени владельца сертификата Центр Регистрации обеспечивает уникальность имени пользователя в системе.

Примечание:

В случае невозможности личного присутствия Пользователя, либо лица им уполномоченного, в Удостоверяющем центре, лицензия регистрации пользователя и ключ регистрации доставляются Пользователю доверенным способом.

7.7 При наличии системы электронной почты и зарегистрированного почтового адреса пользователя, администратор УЦ добавляет его в список рассылки пользователей системы, который используется для централизованного оповещения пользователей системы;

7.8 Ключ и лицензия регистрации пользователя.

При формировании ключа электронной подписи, ключа регистрации, сертификата ключа проверки электронной подписи и лицензии регистрации пользователя предлагается использовать следующие значения.

- срок действия ключа электронной подписи пользователя– 1 год 3 месяца;
- срок действия сертификата ключа проверки электронной подписи (лицензии регистрации) пользователя – 5 лет;
- срок действия ключа регистрации пользователя – 1 месяц;

В результате регистрации Пользователь получает:

- ключ регистрации;
- Лицензию регистрации, содержащую сертификаты Удостоверяющего Центра (Центра Сертификации (ЦС), Центра Регистрации (ЦР) и действующие списки аннулированных (отозванных) сертификатов (САС);

Лицензия регистрации является лицензией на формирование ключевой информации Пользователем.

7.9 Формирование ключей Пользователем

7.9.1 Пользователь формирует собственные ключи электронной подписи и проверки электронной подписи(ЭП), формирует запрос на выпуск соответствующего сертификата и передает запрос на сертификат в Удостоверяющий центр.

При этом Пользователь УЦ выполняет действия согласно эксплуатационно-технической документации на ПО СКЗИ "Верба-OW" и ПО «Справочник сертификатов».

- Пользователь, используя сертификат регистрации и ПО «Справочник сертификатов» согласно эксплуатационно-технической документации (далее - ЭТД), производит формирование персонального справочника пользователя (ПСП), в который добавляется сертификат УЦ. Сертификат ЦР. Лицензия регистрации Пользователя и САС добавляются в локальный справочник Пользователя. ПСП защищается с использованием ключа регистрации Пользователя;
- Пользователь производит формирование личного ключа электронной подписи ЭП и запроса на сертификат, содержащего ключ проверки электронной подписи (ЭП) Пользователя. С ключа электронной подписи Пользователя формируется резервная копия, которая хранится у администратора безопасности (при его наличии)

или у ответственного лица.; формирование нового ключа электронной подписи и ключа проверки электронной подписи Пользователя на рабочем месте осуществляется с использованием ключа и сертификата регистрации, или с использованием действующего (зарегистрированного в УЦ ранее) ключа и сертификата;

- формирование запроса на сертификат осуществляется с использованием информации, содержащейся в сертификате регистрации или действующем сертификате;
- формирование ЭП запроса на сертификат производится на вновь изготовленном ключе электронной подписи Пользователя;
- запрос на сертификат в электронной форме передается в Удостоверяющий центр (Центр регистрации). При этом запрос записывается и передается в формате упакованных данных (PKCS#7 Signed с использованием ключа и сертификата регистрации или действующего ключа электронной подписи и сертификата Пользователя). По желанию Пользователь может создать дополнительные (резервные ключи и получить на них сертификат- это обеспечивает «бесперебойность» работы Пользователя при компрометации и/или плановой смене ключей). При наличии сетевого взаимодействия организации с Удостоверяющим центром (Центром регистрации), а так же наличии ПО, поддерживающего обмен электронной почтой по протоколу SMTP, запрос на сертификат может быть передан в Удостоверяющий центр (Центр регистрации) с использованием электронной почты. При этом запрос записывается и передается в формате упакованных данных с использованием ЭП на ключе регистрации пользователя (или действующем ключе электронной подписи). При отсутствии сетевого взаимодействия организации с Удостоверяющим центром (Центром регистрации), запрос записывается на машиночитаемый носитель в формате упакованных данных с использованием ЭП на ключе регистрации пользователя (или действующем ключе электронной подписи). Если запрос был записан на машиночитаемый носитель, Пользователь (администратор безопасности) прибывает в Удостоверяющий центр вместе с записанным запросом;
- При получении запроса на сертификат администратор УЦ производит формирование "шаблона" сертификата пользователя, используя для этого данные, содержащиеся в лицензии регистрации пользователя. При формировании "шаблона" Центр регистрации не имеет права изменять зарегистрированные дополнения сертификата, которые могут повлечь нарушения при функционировании сертификата в прикладной системе. Центр регистрации при формировании сертификата пользователя:

- может изменить срок действия ключа проверки электронной подписи пользователя;
- может изменить срок действия сертификата пользователя;
- может изменить поля дополнения **Альтернативное Имя Владельца**, за исключением тех, которые относятся к функционированию сертификата в прикладной системе;
- может добавить значения одного или нескольких идентификаторов в дополнение **Расширенная область применения ключа** (**extendedKeyUsage**), если это необходимо технологическим процессом обработки прикладной системы для разделения полномочий владельцев сертификатов;
- должен установить в поле Регламент использования сертификата пользователя значение, определяющее прикладную систему, в которой будет использован сертификат;

7.9.2 Администратор ЦР передает сформированный "шаблон" сертификата в Центр сертификации. ЦС производит верификацию "шаблона" (проверив ЭП ЦР) и формирует сертификат пользователя. Сертификат пользователя хранится в базе ЦС в течение установленного срока хранения (равного сроку действия сертификата);

7.9.3 По требованию пользователя администратор ЦР выводит на принтер бланк сертификата пользователя (Приложение №4). Бланк сертификата заверяется подписью администратора (уполномоченного лица) Удостоверяющего центра. Подписанный бланк сертификата передается пользователю. Удостоверяющий Центр обязан подготовить личный сертификат Пользователя в течение 2 (двух) рабочих дней с момента получения запроса.

7.9.4 Получение личного сертификата пользователем.

Личный сертификат может быть получен следующими способами:

- при личном присутствии пользователя (администратора безопасности) в Удостоверяющем центре (Центре регистрации);
- по электронной почте, если в сертификате пользователя есть зарегистрированный адрес электронной почты.

Примечание.

При получении квалифицированного сертификата Администратор Удостоверяющего центра под расписку ознакамливает пользователя с информацией, содержащейся в квалифицированном сертификате. При невозможности личного присутствия пользователя или его представителя в Удостоверяющем центре, расписка может быть направлена пользователем по почте, а при наличии электронного взаимодействия расписка может быть представлена в виде электронного документа с электронной подписью пользователя.

Одновременно с выдачей квалифицированного сертификата пользователь получает выписку из нормативных документов, регламентирующих. порядок обращения с СКЗИ и криптоключами к ним

Администратор УЦ производит публикацию сертификата пользователя в реестре сертификатов.

Реестр сертификатов доступен пользователям по адресу: http://www.security.ru/com_cer/index.php

При получении личного сертификата, Пользователь производит его добавление в раздел справочника **Личные сертификаты**, используя ПО **Справочник сертификатов.**

7.10 Повторная регистрация пользователя.

Повторная регистрация Пользователя в Центре регистрации производится в случае изменения зарегистрированных атрибутов Пользователя по инициативе Пользователя либо Центра регистрации.

7.11 Обновление сертификата Пользователя.

Обновление сертификата Пользователя может быть вызвано следующими причинами:

- окончанием срока действия ключа электронной подписи;
- окончанием срока действия сертификата.

Формирование нового ключа электронной подписи, запроса на сертификат, передача запроса в Удостоверяющий центр (Центр регистрации) и получение сертификата производится согласно последовательности, описанной в п.п. 7.9.1-7.9.4 настоящего Регламента, за исключением необходимости формирования ПСП Пользователя.

Обновление сертификата не допускает изменения данных Пользователя, включенных в сертификат регистрации.

В случае необходимости изменения регистрационных данных, Пользователь обязан провести повторную регистрацию.

7.12 Плановая смена ключей Пользователя УЦ.

Пользователь, имеющий действующий сертификат и соответствующий ему ключ электронной подписи ЭП, в любой момент времени (но не позднее недели) до окончания срока действия действующего ключа электронной подписи, может произвести формирование нового ключа электронной подписи.

Формирование нового ключа электронной подписи, запроса на сертификат, передача запроса в Удостоверяющий центр (Центр регистрации) и получение сертификата производится согласно последовательности, описанной в п.п. 7.9.1-7.9.4 настоящего Регламента, за исключением необходимости формирования ПСП Пользователя.

7.13 Формирование ключей Пользователя Удостоверяющим центром.

Удостоверяющий центр создает ключи электронных подписей по обращению Пользователя с гарантией сохранения в тайне ключа электронной подписи Пользователя.

Регистрация Пользователей в Удостоверяющем центре выполняется в соответствии с порядком, изложенным в пп. 7.1-7.5

После регистрации Пользователя Администратор УЦ производит формирование:

- Лицензии регистрации;
- ключа электронной подписи;
- Сертификата пользователя;

По требованию пользователя администратор УЦ выводит на принтер бланк сертификата пользователя (Приложение №4). Бланк сертификата заверяется подписью администратора (уполномоченного лица) Удостоверяющего центра. Подписанный бланк сертификата передается пользователю.

Зарегистрированный Пользователь получает:

- Ключ электронной подписи на ключевом носителе Пользователя, поддерживаемом СКЗИ «Верба»;

- Сертификат пользователя;
- Копию базы справочника пользователя;

В бумажной форме:

Заверенный бланк сертификата Пользователя УЦ (по требованию пользователя);

Примечания:

1. Ключ электронной подписи Пользователя по согласованию с ним может быть записан на машиночитаемый носитель, предоставляемый администратором ЦР.
2. Сертификат пользователя и копия базы справочника пользователя могут быть получены Пользователем в порядке, оговоренном в п.п.7.9.4, либо записаны на машиночитаемый носитель (дискету), предоставляемый администратором УЦ.
3. При Обновлении сертификата Пользователя и Плановой смене ключей Пользователя УЦ формирование запроса на сертификат осуществляется Удостоверяющим Центром. При этом Бланк запроса на сертификат на принтер не выводится.

7.14 Компрометация ключей Пользователя УЦ.

При компрометации ключа у Пользователя он должен немедленно прекратить связь по сети с другими пользователями.

Пользователь (или администратор безопасности организации) должен немедленно известить Удостоверяющий центр (Центр регистрации) о компрометации ключей Пользователя.

При наличии сетевого взаимодействия Пользователь может оповестить Удостоверяющий центр (Центр регистрации) путем формирования электронного сообщения о компрометации с использованием ПО «Справочник сертификатов» и передачей его в Удостоверяющий центр (Центр регистрации).

После компрометации ключей Пользователь формирует новый ключ электронной подписи и запрос на сертификат. Так как Пользователь не может использовать скомпрометированный ключ для формирования ЭП и передачи запроса в защищенном виде по сети, запрос на сертификат (на машиночитаемом носителе) доставляется лично или через специальную почтовую связь Пользователем (администратором безопасности) в Центр Регистрации.

7.15 Действия Удостоверяющего центра при компрометации ключей Пользователя.

При получении сообщения о компрометации ключа Пользователя, Удостоверяющий центр не позднее 1 (одного) рабочего дня, следующего за рабочим днем, в течение которого было подано заявление, обеспечивает добавление сертификата, соответствующего) ключу электронной подписи в список аннулированных (отозванных) сертификатов.

Дата и время, с которой сертификат считается недействительным в системе, устанавливается равной дате и времени изготовления САС, в который был включен отзываемый сертификат.

При наличии сетевых средств распространения САС, администратор УЦ производит публикацию САС.

Для распространения САС может быть использована электронная почта, с использованием которой ЦР рассылает вновь изданный САС, всем пользователям, зарегистрированным в списке рассылки.

Сертификат ключа проверки электронной подписи Пользователя не удаляется из базы ЦР и хранится в течение 10 (десяти) лет для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

7.16 Исключение Пользователя УЦ из Удостоверяющего центра (аннулирование сертификата ключа проверки электронной подписи Пользователя).

Исключение Пользователя из УЦ может быть осуществлено на основании письменного заявления Пользователя УЦ в адрес руководителя Удостоверяющего Центра, (Приложение №5,6) заверенного Пользователем Исключение Пользователя из УЦ аналогично компрометации ключа Пользователя. Получив такое заявление, администратор УЦ производит действия, описанные в п.7.15, .

7.17 Порядок разбора конфликтных ситуаций, связанных с применением ЭП.

Применение электронной подписи в автоматизированной системе может приводить к конфликтным ситуациям, заключающимся в оспаривании сторонами (участниками системы) авторства и/или содержимого документа, подписанного электронной подписью.

Разбор подобных конфликтных ситуаций в соответствии с действующим законодательством и особенностями формирования самой электронной подписи требует применения специального программного обеспечения для выполнения проверок и документирования данных, используемых при выполнении процедуры проверки соответствия ЭП содержимому электронного документа.

Разбор конфликтной ситуации заключается в доказательстве авторства подписи конкретного электронного документа конкретным исполнителем.

Данный разбор основывается на математических свойствах алгоритма ЭП, реализованного в соответствии со стандартами Российской Федерации, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, гарантирующими невозможность подделки значения ЭП любым лицом, не обладающим) ключом электронной подписи.

При проверке значения ЭП используется ключ проверки электронной подписи, значение которого вычисляется по значению ключа ЭП при их формировании.

Система криптографической защиты информации позволяет выполнять проверку значения ЭП в течение установленного в системе срока хранения ключей проверки электронных подписей электронных документов, для чего в системе должны быть предусмотрены средства ведения архивов электронных документов с ЭП и сертификатов ключей проверки электронных подписей.

Разбор конфликтной ситуации выполняется комиссией, состоящей из представителей сторон и экспертов.

Оспаривание результатов работы комиссии и возмещение пострадавшей стороне принесенного ущерба выполняется в установленном действующим законодательством Российской Федерации порядке.

7.17.1 Порядок разбора конфликтной ситуации.

Разбор конфликтной ситуации выполняется по инициативе любого участника автоматизированной системы и состоит из:

- предъявления претензии одной стороны другой;
- формирования комиссии;
- разбора конфликтной ситуации;
- взыскания с виновной стороны принесенного ущерба.

Разбор конфликтной ситуации проводится с использованием ПО Программного комплекса разбора конфликтных ситуаций, входящего в состав ПК Центр регистрации для электронного документа, авторство или содержание которого оспаривается.

Протокол проверки ЭП, формируемый данной программой, является основным документом работы комиссии и должен быть подписан всеми членами комиссии.

Проверка подписанного электронного документа включает в себя выполнение следующих действий:

- определение сертификата, необходимого для проверки ЭП;
- проверка ЭП электронного документа с использованием сертификата;
- определение даты формирования каждой ЭП в электронном документе;
- проверка ЭП сертификата;
- проверка действительности сертификата на текущий момент времени;
- проверка действительности сертификата на момент формирования ЭП;
- проверка отсутствия сертификата в САС.

Если сертификат, с использование которого проверяется ЭП, отозван, комиссия принимает решение о действительности ЭП документа, используя дату создания документа и дату отзыва сертификата в САС.

При успешной проверке ЭП документа и верификации сертификата, отсутствии сертификата в САС, авторство подписи под документом считается установленным.

Примечание.

Несовпадение даты формирования документа и сроков действия сертификата и/или сроков действия ключа электронной подписи **не влияют** на определение авторства документа. На их основе можно сделать предположение о несоблюдении пользователем Регламента в части сроков действия ключей, сертификатов или некорректного использования сертификата в прикладном ПО.

7.17.2 Случаи невозможности проверки значения ЭП

При необнаружении в архиве (базе) сертификата ключа проверки электронной подписи пользователя, выполнившего ЭП, доказать авторство документа невозможно. В связи с этим, архив с сертификатами ключей проверки электронных подписей необходимо подвергать регулярному резервному копированию и хранить в течение всего установленного срока хранения.

8. Дополнительные положения.

8.1 Плановая смена ключа электронной подписи Удостоверяющего центра

В течение двух месяцев до окончания срока действия ключа электронной подписи Удостоверяющего центра администратор УЦ производит формирование нового ключа электронной подписи и сертификата ключа проверки электронной подписи УЦ

Срок начала действия ключа электронной подписи во вновь изготовленном сертификате устанавливается равным сроку окончания действия ключа электронной подписи в действующем сертификате. Срок начала действия сертификата устанавливается равным сроку началу действия ключа электронной подписи. УЦ.

Администратор УЦ публикует новый сертификат ключа проверки электронной подписи УЦ (в der кодировке) по адресу:

http://www.security.ru/ca/mo_accredited.cer.

Все Пользователи, эксплуатирующие прикладное ПО, включающее в себя ПО «Справочник сертификатов» во время, оставшееся до окончания срока действия ключа электронной подписи УЦ (ключа Центра сертификации УЦ), обязаны получить новый сертификат ключа Центра сертификации УЦ и добавить его в ПСП с использованием ПО «Справочник сертификатов» без удаления действующего сертификата ключа Центра сертификации УЦ.

8.2 Плановая смена ключа электронной подписи УЦ (ключа Центра регистрации УЦ). В течение двух месяцев до окончания срока действия ключа электронной подписи УЦ администратор УЦ производит формирование нового ключа электронной подписи и сертификата ключа проверки электронной подписи УЦ

Смена ключа Центра регистрации УЦ производится аналогично смене ключей Пользователя.

Все Пользователи, эксплуатирующие прикладное ПО, включающее в себя ПО «Справочник сертификатов» во время, оставшееся до окончания срока действия ключа электронной подписи УЦ (ключа электронной подписи ЦР), обязаны получить новый сертификат УЦ (сертификат Центра регистрации УЦ) .

8.3 Компрометация ключей Центра сертификации и Центра регистрации.

8.3.2 По факту компрометации ключей должно быть проведено служебное расследование. Выведенные из действия, скомпрометированные ключевые носители после проведения служебного расследования уничтожаются.

Компрометация ключа Центра сертификации УЦ.

В случае компрометации ключа Центра сертификации УЦ вся система должна быть остановлена.

При наличии резервных ключей, система должна полностью перейти на комплект резервных ключей.

Если резервные ключи не были предусмотрены, для восстановления системы необходимо: повторно произвести формирование ключа и сертификата ЦС; сформировать САС ЦС, с указанием в нем отзываемого сертификата ЦС; обеспечить получение сертификата и САС ЦС всеми пользователями системы; произвести выпуск новых сертификатов всех пользователей, используя действующие сертификаты; обеспечить получение новых личных сертификатов пользователями системы.

8.3.3 Компрометация ключа Центра регистрации УЦ

Компрометация ключа Центра регистрации УЦ не приводит к останову системы. В случае компрометации становится невозможным сетевой взаимодействие между пользователем системы и ЦР в части управления ключевой системой.

В случае компрометации ключа Центра регистрации УЦ должны быть выполнены следующие мероприятия:

- ЦС формирует САС, с указанием в нем отзываемого сертификата Центра регистрации УЦ;
- при наличии резервных ключей ЦР, ЦР переходит на резервный ключ.

Если резервные ключи не были предусмотрены, для восстановления системы необходимо:

- повторно произвести формирование ключа и сертификата ЦР;

обеспечить получение сертификата ЦР всеми пользователями системы (в случае сетевого взаимодействия).

8.4 Периодичность издания Списка отозванных сертификатов.

Периодичность издания САС (приложение № 4 к настоящему Регламенту) обеспечивается Центром сертификации. Период обновления САС составляет 300 дней.

При этом Удостоверяющий центр обеспечивает публикацию САС по адресу: http://www.security.ru/ca/mo_accredited.crl

В случае поступления сообщения Пользователя о компрометации, обновление САС и публикация его в точке публикации производится не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было получено сообщение о компрометации.

Для распространения вновь изданного САС, может быть использована система электронной почты и список рассылки пользователей системы, который формируется при регистрации пользователей.

Пользователь, должен регулярно в соответствии с принятой политикой безопасности и настройками своего рабочего места обновлять САС, хранящийся в локальном справочнике сертификатов с использованием ПО «Справочник сертификатов».

8.5 Хранение сертификатов ключей проверки электронных подписей в Удостоверяющем Центре.

Срок хранения сертификата ключа проверки электронной подписи Пользователя в Удостоверяющем Центре осуществляется в течение всего периода его действия и 5 (Пять) лет после его аннулирования (отзыва). По истечении указанного срока хранения сертификаты ключей проверки электронной подписи переводятся в режим архивного хранения.

8.6 Архивное хранение.

8.6.1 Документы, подлежащие архивному хранению.

Архивному хранению подлежат следующие документы Удостоверяющего Центра:

- аннулированные сертификаты ключей проверки электронной подписи Удостоверяющего центра;
- аннулированные сертификаты пользователей Удостоверяющего Центра;
- заявления на регистрацию пользователей в Удостоверяющем Центре;
- заявления на аннулирование (отзыв) сертификатов ключей проверки электронных подписей;
- служебные документы Удостоверяющего Центра.

Документы Удостоверяющего Центра на бумажных носителях, в том числе и сертификаты ключей проверки электронной подписи пользователей на бумажном носителе, хранятся в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

8.6.2 Срок архивного хранения.

Документы, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов – 5 (Пять) лет.

8.6.3 Уничтожение архивных документов.

Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией, формируемой из числа сотрудников Удостоверяющего Центра.

8.7 Структура сертификатов ключей электронной подписи и списков отозванных сертификатов.

Удостоверяющий Центр издает сертификаты ключей проверки электронной подписи Пользователей УЦ в электронной форме формата X.509 версии 3.

– Издаваемые Удостоверяющим Центром квалифицированные сертификаты соответствуют требованиям Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" и Приказу ФСБ РФ от 27.12.2011 N 795"Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи".

Удостоверяющий Центр издает CAC формата X.509 версии 2.

Поддерживаются следующие дополнения CAC:

– идентификатор ключа ЦС (authority KeyIdentifier);
– номер CAC.

Для записи об отзыве поддерживаются следующие дополнения:

– код причины отзыва;
– дата отзыва.

Примеры распечаток сертификата Центра сертификации, и сертификатрв пользователей приведены ниже.

Инфраструктура открытых ключей VCERT MV

Сертификат корневого Центра Сертификации

Данные:
Версия: 3 (0x2)
Серийный Номер:40:00:00:00:01:FB:E8:D4:4F:E1:AC:C8:00:FE:36:CB
Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
Издатель: CN=УЦ ЗАО МО ПНИЭИ,O=МО ПНИЭИ,streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2,
ST=77 Москва,L=г. Москва,C=ru,Email=mopniei@mo.msk..ru,INN=123456789012,OGRN=1234567890123
Срок действия
Действителен с: 20 Июн 2012 10:57:00 GMT
Действителен по: 20 Июн 2017 23:59:00 GMT
Владелец: CN=УЦ ЗАО МО ПНИЭИ,O=МО ПНИЭИ,streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2,
ST=77 Москва,L=г. Москва,C=ru,Email=mopniei@mo.msk..ru,INN=123456789012,OGRN=1234567890123
Открытый Ключ Владельца:
Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
Открытый ключ ГОСТ Р 34.10-2001:
Параметры алгоритма:
Параметры открытого ключа: Параметры ГОСТ Р 34.10-2001 вариант провайдера
Параметры хэширования: Узел замены для хэша вариант провайдера
длина ключа: 512 бит
54:5B:DD:95:F1:FA:D8:7A:CF:40:B7:03:20:7C:65:87:
F4:6E:06:D9:C2:34:08:D6:50:F1:2B:F7:B0:9B:AC:70:
FD:BF:34:72:FD:A9:C4:CC:F7:66:DD:83:96:9F:CF:5F:
71:BC:AB:EC:26:41:9B:5F:34:FB:47:3F:28:F0:9B:62

Дополнения X.509:
X509v3 Срок Действия Закрытого Ключа:
Действителен с:20 Июн 2012 10:57:00 GMT
Действителен по:20 Сен 2013 23:59:00 GMT
Средство ЭП Владельца:
СКЗИ Верба-OW (версия 6.1.2)
X509v3 Область Применения Ключа:
Электронная Подпись
Подпись Сертификата
Подпись COC
X509v3 Политики Сертификата:
Идентификатор Политики: 1.2.643.100.113.1 - класс средств ЭП КС1
Идентификатор Политики: 1.2.643.100.113.2 - класс средств ЭП КС2
Средства ЭП и УЦ Издателя:
Средство электронной подписи:
СКЗИ Верба-OW (версия 6.1.2)
Средство УЦ:
Удостоверяющий центр АПК Верба-сертификат МВ версия 2.0
Заключение на средство ЭП: СФ/124-1499 от 30.04 2010г.
Заключение на средство УЦ: СФ/128-1500 от 22.06 2010г.
Идентификатор Закрытого ключа:
Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
Идентификатор Закрытого ключа: 2995YSK67K01
X509v3 Идентификатор Ключа Владельца:
C2:9C:5A:F3:06:B3:DC:E8:D9:2A:E8:CB:79:1D:2A:71:A1:EA:AA:8B
X509v3 Основные Ограничения: критичное
CA:TRUE
pathlen:4

Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
CE:F8:21:54:13:C5:8C:C3:94:4F:34:E2:16:ED:D8:88:
75:70:D6:59:5B:EA:85:79:62:0B:25:D5:C3:F3:98:94:
12:EE:F1:1C:56:BD:4E:DB:A3:22:81:09:2D:98:D1:84:
C5:3B:A3:22:14:E8:0E:D0:E5:63:C6:A3:67:29:60:1F

Инфраструктура открытых ключей VCERT MV

Уполномоченное лицо

_____ "____" _____ **201__ г.**

М.П.

Полномочный представитель организации:
(владелец сертификата ключа электронной подписи)

_____ "____" _____ **201__ г.**

Инфраструктура открытых ключей VCERT MV

Сертификат Центра Сертификации

Данные:
Версия: 3 (0x2)
Серийный Номер:40:00:00:00:54:B2:43:81:4F:E1:AE:19:01:03:5A:A7
Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
Издатель: CN=УЦ ЗАО МО ПНИЭИ,O=МО ПНИЭИ,streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2,
ST=77 Москва,L=г. Москва,C=ru,Email=mopniei@mo.mak..ru,INN=123456789012,OGRN=1234567890123
Срок действия
Действителен с: 20 Июн 2012 11:03:55 GMT
Действителен по: 20 Июн 2017 23:59:00 GMT
Владелец: CN=УЦ (2),O=МО ПНИЭИ,streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2,ST=77
Москва,L=г. Москва,C=ru,Email=mopniei@mo.msk.ru,INN=123456789012,OGRN=1234567890123
Открытый Ключ Владельца:
Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
Открытый ключ ГОСТ Р 34.10-2001:
Параметры алгоритма:
Параметры открытого ключа: Параметры ГОСТ Р 34.10-2001 вариант провайдера
Параметры хэширования: Узел замены для хэша вариант провайдера
длина ключа: 512 бит
D9:DD:7D:9A:3C:E9:7D:54:B2:3B:73:D3:D7:7E:E1:99:
38:AA:F2:4D:EC:1A:A9:5C:B8:6D:FF:AA:6E:7B:9D:22:
3F:70:27:14:94:18:3F:49:AB:13:DB:6C:F5:B6:02:4F:
5D:DC:45:61:72:C4:67:32:16:01:EB:35:69:63:D8:DF

Дополнения X.509:
Средство ЭП Владельца:
СКЗИ Верба-OW (версия 6.1.2)
Средства ЭП и УЦ Издателя:
Средство электронной подписи:
СКЗИ Верба-OW (версия 6.1.2)
Средство УЦ:
Удостоверяющий центр АПК Верба-сертификат МВ версия 2.0
Заключение на средство ЭП: СФ/124-1499 от 30.04 2010г.
Заключение на средство УЦ: СФ/128-1500 от 22.06 2010г.
Ссылка на Сертификат Регистрации:
Идентификатор ключа:9C:DA:F5:19:FB:35:4D:90:05:F2:01:C3:44:44:32:E6:B7:1B:63:42
Имя в директории:OGRN=1234567890123/INN=123456789012/Email=mopniei@mo.msk..ru/C=ru/L=г.
Москва/ST=77 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=УЦ
ЗАО МО ПНИЭИ
Серийный номер:40:00:00:00:52:51:B8:14:4F:E1:AD:73:01:00:D3:21
X509v3 Идентификатор Ключа Владельца:
A3:3D:71:4F:F5:6E:6D:51:47:B6:6A:86:E9:A2:94:14:85:1F:86:88
Ссылка на предыдущий сертификат:
Идентификатор ключа:9C:DA:F5:19:FB:35:4D:90:05:F2:01:C3:44:44:32:E6:B7:1B:63:42
Имя в директории:OGRN=1234567890123/INN=123456789012/Email=mopniei@mo.msk..ru/C=ru/L=г.
Москва/ST=77 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=УЦ
ЗАО МО ПНИЭИ
Серийный номер:40:00:00:00:52:51:B8:14:4F:E1:AD:73:01:00:D3:21
Идентификатор Закрытого ключа:
Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
Идентификатор Закрытого ключа: 3818A7P2MP01
X509v3 Область Применения Ключа:
Электронная Подпись
Подпись Сертификата
Подпись СОС
X509v3 Срок Действия Закрытого Ключа:
Действителен с:20 Июн 2012 11:03:55 GMT
Действителен по:20 Июн 2013 23:59:00 GMT
X509v3 Политики Сертификата:
Идентификатор Политики: 1.2.643.100.113.1 - класс средств ЭП КС1
Идентификатор Политики: 1.2.643.100.113.2 - класс средств ЭП КС2
X509v3 Идентификатор Ключа Издателя:
Идентификатор ключа:C2:9C:5A:F3:06:B3:DC:E8:D9:2A:E8:CB:79:1D:2A:71:A1:EA:AA:8B
Имя в директории:OGRN=1234567890123/INN=123456789012/Email=mopniei@mo.msk..ru/C=ru/L=г.
Москва/ST=77 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=УЦ
ЗАО МО ПНИЭИ
Серийный номер:40:00:00:00:01:FB:E8:D4:4F:E1:AC:C8:00:FE:36:CB
X509v3 Основные Ограничения: критичное
CA:TRUE
pathlen:0

Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
8B:55:EF:BC:4D:C4:0F:FE:CD:90:46:22:85:DF:13:AF:

Инфраструктура открытых ключей VCERT MV

```
F1:C4:DA:28:E1:82:93:14:36:75:46:5C:90:C8:E3:1E:
50:25:D8:BA:23:FA:DD:F3:71:64:34:20:71:B1:5A:EB:
B0:EA:89:3B:B1:8E:E0:6E:E7:2F:8E:26:D1:16:6D:F3
```

Уполномоченное лицо

_____"____"_____**201__г.**

М.П.

Полномочный представитель организации:
(владелец сертификата ключа электронной подписи)

_____"____"_____**201__г.**

Инфраструктура открытых ключей VCERT MV

Сертификат

Данные:
Версия: 3 (0x2)
Серийный Номер:40:00:00:00:2C:E8:C6:82:4F:E1:B2:4C:01:13:C1:33
Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
Издатель: CN=УЦ (2),O=МО ПНИЭИ,streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2,ST=77
Москва,L=г. Москва,C=ru,Email=mopniei@mo.msk.ru,INN=123456789012,OGRN=1234567890123
Срок действия
Действителен с: 20 Июн 2012 11:21:50 GMT
Действителен по: 20 Июн 2017 23:59:00 GMT
Владелец: CN=Иванов Иван Иванович,O=ИЧП,streetAddress=ул. Беговая д.1,ST=77 Москва,L=г.
Москва,C=ru,INN=123456789012,SNILS=12345678901,OGRNIP=123456789012345
Открытый Ключ Владельца:
Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
Открытый ключ ГОСТ Р 34.10-2001:
Параметры алгоритма:
Параметры открытого ключа: Параметры Диффи-Хеллман вариант провайдера
Параметры хэширования: Узел замены для хэша вариант провайдера
длина ключа: 512 бит
43:6D:68:60:8B:13:C2:3C:8C:3D:D5:FF:D8:D6:B9:36:
37:5D:21:DD:A4:13:AF:14:5A:87:FB:75:E7:0D:E2:38:
46:D4:18:54:92:25:1F:71:A2:E1:C8:E9:E6:0F:B4:BC:
17:E0:4F:5F:9B:5E:BB:E4:24:04:65:6C:4B:32:88:31

Дополнения X.509:
Средство ЭП Владельца:
СКЗИ Верба-OW (версия 6.1.2)
Ссылка на Сертификат Регистрации:
Идентификатор ключа:D6:F8:BD:3C:50:1A:4A:01:48:3D:40:E7:80:99:9F:9C:B4:7F:96:D4
Имя в директории:OGRN=1234567890123/INN=123456789012/C=ru/L=г.Москва/ST=77
Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=ЦР(2)
Серийный номер:40:00:00:00:9C:21:84:10:4F:E1:B2:43:01:13:9D:FB
X509v3 Идентификатор Ключа Владельца:
E4:90:5F:B4:56:EF:5E:E2:21:C2:FA:34:38:A7:AE:AC:15:F6:40:FA
Ссылка на предыдущий сертификат:
Идентификатор ключа:D6:F8:BD:3C:50:1A:4A:01:48:3D:40:E7:80:99:9F:9C:B4:7F:96:D4
Имя в директории:OGRN=1234567890123/INN=123456789012/C=ru/L=г.Москва/ST=77
Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=ЦР(2)
Серийный номер:40:00:00:00:9C:21:84:10:4F:E1:B2:43:01:13:9D:FB
Идентификатор Закрытого ключа:
Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
Идентификатор Закрытого ключа: 2150S8IDCW01
Ключ выработан в Центре Регистрации:
X509v3 Область Применения Ключа:
Электронная Подпись
Неотрекаемый
Шифрование Ключа
Шифрование Данных
X509v3 Срок Действия Закрытого Ключа:
Действителен с:20 Июн 2012 11:21:50 GMT
Действителен по:20 Сен 2013 23:59:00 GMT
Средства ЭП и УЦ Издателя:
Средство электронной подписи:
СКЗИ Верба-OW (версия 6.1.2)
Средство УЦ:
Удостоверяющий центр АПК Верба-сертификат МВ версия 2.0
Заключение на средство ЭП: СФ/124-1499 от 30.04 2010г.
Заключение на средство УЦ: СФ/128-1500 от 22.06 2010г.
X509v3 Основные Ограничения: критичное
CA:FALSE
X509v3 Политики Сертификата:
Идентификатор Политики: 1.2.643.100.113.1 - класс средств ЭП КС1
X509v3 Идентификатор Ключа Издателя:
Идентификатор ключа:A3:3D:71:4F:F5:6E:6D:51:47:B6:6A:86:E9:A2:94:14:85:1F:86:88
Имя в директории:OGRN=1234567890123/INN=123456789012/Email=mopniei@mo.msk..ru/C=ru/L=г.
Москва/ST=77 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=УЦ
ЗАО МО ПНИЭИ
Серийный номер:40:00:00:00:54:B2:43:81:4F:E1:AE:19:01:03:5A:A7

Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
47:86:80:67:FA:7D:D1:AE:40:D9:CF:3F:E1:8E:49:81:
F7:A7:D6:AC:42:B1:D1:D5:B0:03:EE:63:1D:54:49:72:
CA:B3:64:5A:0D:1E:46:C2:61:AD:6C:10:33:A0:2D:48:

Инфраструктура открытых ключей VCERT MV

84:C9:A1:E3:53:74:1D:B0:FE:81:94:7F:EA:7F:9B:A0

Уполномоченное лицо

_____"____"_____**201__г.**

М.П.

Полномочный представитель организации:
(владелец сертификата ключа электронной подписи)

_____"____"_____**201__г.**

Инфраструктура открытых ключей VCERT MV

Сертификат

Данные:
Версия: 3 (0x2)
Серийный Номер:40:00:00:00:AB:C9:ED:B7:4F:E1:B3:2A:01:17:26:57
Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
Издатель: CN=УЦ (2),O=МО ПНИЭИ,streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2,ST=77 Москва,L=г. Москва,C=ru,Email=mopniei@mo.msk.ru,INN=123456789012,OGRN=1234567890123
Срок действия
Действителен с: 20 Июн 2012 11:25:32 GMT
Действителен по: 20 Июн 2017 23:59:00 GMT
Владелец: CN=Петров Пётр Петрович,O=Фирма,streetAddress=ул.Беговая д.2,ST=77 Москва,L=г. Москва,C=ru,INN=123456789012,OGRN=1234567890123
Открытый Ключ Владельца:
Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
Открытый ключ ГОСТ Р 34.10-2001:
Параметры алгоритма:
Параметры открытого ключа: Параметры Диффи-Хеллман вариант провайдера
Параметры хэширования: Узел замены для хэша вариант провайдера
длина ключа: 512 бит
56:E1:B7:59:F5:F6:37:D3:90:1B:A2:90:BE:04:E8:44:
08:8E:75:20:0A:F5:90:51:4A:0A:50:DB:26:91:DD:7F:
8D:C5:D1:04:A2:0F:52:99:A9:7A:44:23:A0:C6:B0:EA:
CE:CA:8C:75:6E:99:77:AD:A3:38:EC:2B:7B:04:6F:DE

Дополнения X.509:
Средство ЭП Владельца:
СКЗИ Верба-OW (версия 6.1.2)
Ссылка на Сертификат Регистрации:
Идентификатор ключа:AF:D5:B9:72:76:55:42:85:88:86:E7:10:33:D2:CA:81:B3:B3:2E:FB
Имя в директории:OGRN=1234567890123/INN=123456789012/C=ru/L=г.Москва/ST=77 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=ЦР(2)
Серийный номер:40:00:00:00:13:9E:D5:57:4F:E1:B3:23:01:17:0A:D0
X509v3 Идентификатор Ключа Владельца:
EC:EA:74:96:B3:6B:39:F8:F3:7D:34:BE:6F:9E:CE:AF:57:55:C4:6F
Ссылка на предыдущий сертификат:
Идентификатор ключа:AF:D5:B9:72:76:55:42:85:88:86:E7:10:33:D2:CA:81:B3:B3:2E:FB
Имя в директории:OGRN=1234567890123/INN=123456789012/C=ru/L=г.Москва/ST=77 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=ЦР(2)
Серийный номер:40:00:00:00:13:9E:D5:57:4F:E1:B3:23:01:17:0A:D0
Идентификатор Закрытого ключа:
Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
Идентификатор Закрытого ключа: 8083SIC3XX01
Ключ выработан в Центре Регистрации:
X509v3 Область Применения Ключа:
Электронная Подпись
Неотрекаемый
Шифрование Ключа
Шифрование Данных
X509v3 Срок Действия Закрытого Ключа:
Действителен с:20 Июн 2012 11:25:32 GMT
Действителен по:20 Сен 2013 23:59:00 GMT
Средства ЭП и УЦ Издателя:
Средство электронной подписи:
СКЗИ Верба-OW (версия 6.1.2)
Средство УЦ:
Удостоверяющий центр АПК Верба-сертификат МВ версия 2.0
Заключение на средство ЭП: СФ/124-1499 от 30.04 2010г.
Заключение на средство УЦ: СФ/128-1500 от 22.06 2010г.
X509v3 Основные Ограничения: критичное
CA:FALSE
X509v3 Политики Сертификата:
Идентификатор Политики: 1.2.643.100.113.2 - класс средств ЭП КС2
X509v3 Идентификатор Ключа Издателя:
Идентификатор ключа:A3:3D:71:4F:F5:6E:6D:51:47:B6:6A:86:E9:A2:94:14:85:1F:86:88
Имя в директории:OGRN=1234567890123/INN=123456789012/Email=mopniei@mo.msk..ru/C=ru/L=г. Москва/ST=77 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=УЦ ЗАО МО ПНИЭИ
Серийный номер:40:00:00:00:54:B2:43:81:4F:E1:AE:19:01:03:5A:A7

Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
FA:A7:E2:AE:8E:A6:9B:36:CD:14:C2:09:78:49:EC:73:
70:D1:A2:01:5B:20:1B:F6:F3:49:0F:6F:C2:15:11:DE:
CD:B7:E2:36:D7:67:94:3D:33:B3:FD:D2:D1:3A:2D:50:

Инфраструктура открытых ключей VCERT MV

74:65:18:21:E8:1A:F6:8B:6E:5F:E3:4B:63:72:4B:C0

Уполномоченное лицо

_____"____"_____**201__г.**

М.П.

Полномочный представитель организации:
(владелец сертификата ключа электронной подписи)

_____"____"_____**201__г.**

8.8 Установление доверительных отношений между УЦ ЗАО МО ПНИЭИ и УЦ внешних организаций

Установление доверительных отношений между двумя УЦ является организационно-технической процедурой, в результате которой пользователи корпоративных информационных систем и информационных систем общего пользования, получившие сертификаты ключей проверки электронных подписей (далее сертификаты) в одном УЦ, получают возможность проверить подлинность ЭП в электронных документах пользователей информационных систем, получивших сертификаты в другом УЦ.

Для установления доверительных отношений каждая из Сторон (УЦ ЗАО МО ПНИЭИ и УЦ внешней организации) передает сертификаты ключей проверки электронных подписей корневого УЦ и подчиненных УЦ, которыми будут заверяться ключи электронных подписей пользователей, зарегистрированных в данном УЦ и в подчиненных УЦ и оформляет на бумажном носителе «Акт обмена сертификатами ключей проверки электронных подписей Удостоверяющего Центра», К Акту прилагаются распечатанные на бумажных носителях копии сертификатов. Акт подписывается начальником УЦ ЗАО МО ПНИЭИ и руководителем УЦ внешней организации, скрепляется печатями УЦ ЗАО МО ПНИЭИ и УЦ внешней организации, и передается под расписку другой Стороне.

Списки отозванных сертификатов (CAC) и сертификаты УЦ внешней организации в электронном виде передаются в УЦ ЗАО МО ПНИЭИ, а сертификаты УЦ ЗАО МО ПНИЭИ и CAC УЦ ЗАО МО ПНИЭИ в электронном виде передаются в УЦ внешней организации.

В каждом из УЦ производится сравнение электронных сертификатов ключей проверки электронных подписей УЦ другой Стороны с распечатанными сертификатами на бумажных носителях и ввод их в действие..

При любом изменении сертификатов ключей проверки электронных подписей УЦ соответствующая Сторона изготавливает сооветствующие копии сертификатов на бумажном носителе и в электронном виде и передает его другой Стороне.8.9 Порядок взаимодействия УЦ при формировании новых списков отозванных сертификатов, при смене ключей электронных подписей УЦ.

При изменении CAC в случае отзыва или приостановки действия сертификатов пользователей УЦ новый CAC высылается в УЦ каждой из Сторон. Полученные CAC подписываются администратором (уполномоченным лицом) УЦ и размещаются в точках публикации УЦ.

Администраторы УЦ каждой из Сторон обязаны производить периодическую (плановую) замену своих ключей не реже заданного срока действия ключа. В целях обеспечения действительности сертификатов пользователей УЦ, заверенных подписью администратора (уполномоченного лица) соответствующего УЦ, замена ключа электронной подписи УЦ должна быть произведена до окончания его срока действия.

В случае компрометации ключа электронной подписи администратор УЦ обязано:

- немедленно сообщить об этом ответственным лицам УЦ другой Стороны;
- аннулировать сертификат ключа подписи и отправить новые CAC в УЦ другой Стороны;
- сформировать новые ключи подписи и сертификат ключа подписи.

После выполнения указанных действий, выполняются мероприятия в соответствии с подразделом 8.8 настоящего Регламента.

9 Конфидециальность.

9.1 Типы конфиденциальной информации.

Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи Пользователя УЦ является конфиденциальной информацией данного Пользователя УЦ. Удостоверяющий Центр не осуществляет хранение ключей электронных подписей пользователей.

Персональные данные Пользователей УЦ и корпоративная информация Пользователей информационных систем, содержащаяся в Удостоверяющем Центре, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи , считается конфиденциальной.

9.2 Типы информации, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

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

Информация, включаемая в сертификаты ключей проверки электронных подписей Пользователей УЦ и списки отозванных сертификатов, издаваемые Удостоверяющим Центром, не являются конфиденциальными.

Информация, содержащаяся в Регламенте, не считается конфиденциальной.

9.3 Исключительные полномочия Удостоверяющего Центра.

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

10. Обеспечение безопасности.

10.1 Центр Сертификации и Центр регистрации Удостоверяющего Центра размещаются на территории ЗАО «МО ПНИЭИ» в выделенном помещении на отдельных компьютерах по схеме организации рабочих мест персонала.

10.2 Помещения Удостоверяющего Центра оборудованы охранно-пожарной и тревожной сигнализациями. Система охранно-пожарной сигнализации обеспечивает круглосуточную работу. Сигналы тревоги выведены на пульты централизованного наблюдения, установленные в помещениях с круглосуточным режимом работы.

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

10.4 Компьютеры Удостоверяющего Центра подключены к электрическим сетям через источник бесперебойного питания.

10.5 Оконные проемы помещений Удостоверяющего Центра оборудованы жалюзи.

10.6 Ограничение физического доступа посторонних лиц в помещения ЗАО «МО ПНЭИ» и Удостоверяющего Центра осуществляется посредством применения электромеханических средств контроля доступа. Ключи (электронные ключи доступа) от помещения предоставлены сотрудникам Удостоверяющего центра по решению руководителя ЗАО «МО ПНЭИ».

10.7 Системные блоки ПЭВМ с установленным ПО опечатаны специально выделенной для этих целей печатью. Контроль целостности ПО Удостоверяющего Центра осуществляется при каждом запуске компьютеров, в соответствии с рекомендациями и требованиями, изложенными в технической документации на соответствующее ПО.

Для обеспечения информационной безопасности УЦ ЗАО МО ПНИЭИ не допускается подключения вычислительных средств с установленными ПК «Центр сертификации» к техническим средствам сетей общего пользования.

Взаимодействие ПК «Центр регистрации» с клиентской частью через корпоративную сеть связи осуществляется с использованием межсетевого экран не ниже 4 класса защиты по требованиям ФСБ, например: аппаратно-программного комплекса «Цитадель-МЭ» или аппаратного межсетевого экрана “Атликс-МЭ-А”.

Программные комплексы (ПК) «Центр сертификации», «Центр регистрации» и АРМ «Разбор конфликтных ситуаций» должны использоваться только совместно с аппаратно-программной реализацией СКЗИ «Верба–OW» версия 6.1.2 (комплектация 2), предусматривающей обязательное использование сертифицированных ФСБ/ФАПСИ аппаратных модулей доверенной загрузки (АМДЗ) со встроенным аппаратным датчиком случайных чисел (ДСЧ), например: программно-аппаратные комплексы (ПАК) «Аккорд» или ПАК «Соболь».

Приложение № 1 к Регламенту

Форма заявления на
регистрацию Пользователя УЦ
для юридических лиц

Руководителю Удостоверяющего центра
ЗАО МО ПНИЭИ

ЗАЯВЛЕНИЕ О РЕГИСТРАЦИИ

в реестре Пользователей Удостоверяющего Центра ЗАО МО ПНИЭИ, присоединению к Регламенту Удостоверяющего центра и изготовлению сертификата ключа проверки электронной подписи

(для юридического лица)

Настоящим _____
(полное фирменное наименование)
Юридический адрес:
_____
_____,
Почтовый адрес
_____
_____

свидетельство о регистрации № _____ от «___» _____ _____г.,
выдано
_____,
*Подразделение_____
ОГРН_____
ИНН_____
КПП_____
КНО_____
**Регистрационный № в ПФР_____
*** РНС ФСС_____
*** КП ФСС _____
Должность_____
в лице _____

* В случае выпуска сертификата на должностное лицо – сотрудника соответствующего подразделение организации

** Заполняется в случае взаимодействия с органами ПФР

*** Заполняется в случае взаимодействия с органами ФСС

Действующего на основании _____

В соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего Центра ЗАО «МО ПНИЭИ» (далее Регламент), просит зарегистрировать в Реестре пользователей Удостоверяющего Центра и изготовить ключ электронной подписи (вычеркнуть, если не требуется) и сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными. Соглашается с обработкой своих персональных данных ЗАО «МО ПНИЭИ» и признает, что персональные данные, заносимые Удостоверяющим Центром ЗАО «МО ПНИЭИ» в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

С настоящим Регламентом и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Ф.И.О. владельца сертификата	
Должность	
СНИЛС*	
телефон / факс	/
e-mail	

*Рекомендуется указывать согласно Методическим рекомендациям Минкомсвязи по составу квалифицированного сертификата.

Подпись_____ (_____)
(Подпись) *(Расшифровка подписи)*

«___»_____ 200__г

М.П.

(Если лицо действует на основании доверенности, приложить доверенность)

Настоящим подтверждаю, что Заявление о регистрации _____. в реестре Пользователей Удостоверяющего Центра ЗАО МО ПНИЭИ получено.

Руководитель Удостоверяющего Центра _____/_____

«__» _____ 20__г.

М. П.

Приложение №2 к Регламенту

Форма заявления на
регистрацию Пользователя УЦ
для физических лиц
(индивидуальных предпринимателей)

ЗАЯВЛЕНИЕ О РЕГИСТРАЦИИ

в реестре Пользователей Удостоверяющего Центра ЗАО МО ПНИЭИ, присоединению к Регламенту Удостоверяющего центра и изготовлению сертификата ключа проверки электронной подписи

(для физического лица, индивидуального предпринимателя)

От

ФИО_____

Паспорт №_____Серия_____

Выдан_____

СНИЛС_____

*ОГРНИП_____

**ИНН _____

* КНО_____

***Регистрационный № в ПФР_____

*** Индивидуальный Регистрационный № в ПФР_____

****РНС ФСС_____

**** КП ФСС _____

* Заполняется для индивидуального предпринимателя при взаимодействии с ФНС

** Рекомендуется указывать согласно Методическим рекомендациям Минкомсвязи по составу квалифицированного сертификата.

*** Заполняется в случае взаимодействия с органами ПФР

*** Заполняется в случае взаимодействия с органами ПФР

****Заполняется в случае взаимодействия с органами ФСС

В соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего Центра ЗАО «МО ПНИЭИ» (далее Регламент), просит зарегистрировать в Реестре пользователей Удостоверяющего Центра и изготовить ключ электронной подписи (вычеркнуть, если не требуется) и сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными. Соглашается с обработкой своих персональных данных ЗАО «МО ПНИЭИ» и признает, что персональные данные, заносимые Удостоверяющим Центром ЗАО «МО ПНИЭИ» в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Личная подпись _____ _____ / _____

Настоящим подтверждаю, что Заявление о регистрации
_____Ф.И.О._____ в реестре Пользователей Удостоверяющего центра ЗАО МО ПНИЭИ получено.

Руководитель Удостоверяющего Центра _____/_____

«__» _____ 20__г.

М. П.

Приложение № 3 к Регламенту

Форма доверенности лицу, уполномоченному организацией - Пользователем Системы защищенного ЭДО осуществить процедуру регистрации для получения сертификата ключа электронной подписи.

ДОВЕРЕННОСТЬ

г. _____ «_____»_____200__г.

_____ (наименование организации), в лице _____, действующего на основании _____настоящей доверенностью уполномочиваю гр.___ _____, паспорт серии_____ №_____ _____ ,выданный_____ ___, проживающего по адресу (регистрации) :_____ _____, осуществить от имени _____ (наименование организации) следующие действия:

1. Зарегистрировать _____ _____ (Ф.И.О.) в Реестре пользователей Удостоверяющего Центра;
2. получить от Удостоверяющего Центра сертификат ключа проверки электронной подписи , оформленный на имя _____ _____ (Ф.И.О.).

Представитель наделяется правом расписываться в соответствующих документах Удостоверяющего центра для исполнения поручений, определенных настоящей Доверенностью.

Подпись _____ _____ (Ф.И.О. представителя)_ _____ заверяю.

Доверенность выдана сроком на один месяц без права передоверия.

«____» _____ 20__г.

_____ / _____
подпись расшифровка подписи

М. П.

Приложение № 4 к Регламенту

Форма копии сертификата ключа проверки электронной подписи на бумажном носителе.

Инфраструктура открытых ключей VCERT MV

Сертификат

```
Данные:
 Версия: 3 (0x2)
 Серийный Номер:40:00:00:00:AB:C9:ED:B7:4F:E1:B3:2A:01:17:26:57
 Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
 Издатель: CN=УЦ (2),O=МО ПНИЭИ,streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2,ST=77
 Москва,L=г. Москва,C=ru,Email=mopniei@mo.msk.ru,INN=123456789012,OGRN=1234567890123
 Срок действия
     Действителен с: 20 Июн 2012 11:25:32 GMT
     Действителен по: 20 Июн 2017 23:59:00 GMT
 Владелец: CN=Петров Пётр Петрович,O=Фирма,streetAddress=ул.Беговая д.2,ST=77 Москва,L=г.
 Москва,C=ru,INN=123456789012,OGRN=1234567890123
 Открытый Ключ Владельца:
 Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
 Открытый ключ ГОСТ Р 34.10-2001:
  Параметры алгоритма:
   Параметры открытого ключа: Параметры Диффи-Хеллман вариант провайдера
   Параметры хэширования: Узел замены для хэша вариант провайдера
  длина ключа: 512 бит
    56:E1:B7:59:F5:F6:37:D3:90:1B:A2:90:BE:04:E8:44:
    08:8E:75:20:0A:F5:90:51:4A:0A:50:DB:26:91:DD:7F:
    8D:C5:D1:04:A2:0F:52:99:A9:7A:44:23:A0:C6:B0:EA:
    CE:CA:8C:75:6E:99:77:AD:A3:38:EC:2B:7B:04:6F:DE

Дополнения X.509:
 Средство ЭП Владельца:
  СКЗИ Верба-OW (версия 6.1.2)
 Ссылка на Сертификат Регистрации:
  Идентификатор ключа:AF:D5:B9:72:76:55:42:85:88:86:E7:10:33:D2:CA:81:B3:B3:2E:FB
  Имя в директории:OGRN=1234567890123/INN=123456789012/C=ru/L=г.Москва/ST=77
 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=ЦР(2)
  Серийный номер:40:00:00:00:13:9E:D5:57:4F:E1:B3:23:01:17:0A:D0
 X509v3 Идентификатор Ключа Владельца:
  EC:EA:74:96:B3:6B:39:F8:F3:7D:34:BE:6F:9E:CE:AF:57:55:C4:6F
 Ссылка на предыдущий сертификат:
  Идентификатор ключа:AF:D5:B9:72:76:55:42:85:88:86:E7:10:33:D2:CA:81:B3:B3:2E:FB
  Имя в директории:OGRN=1234567890123/INN=123456789012/C=ru/L=г.Москва/ST=77
 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=ЦР(2)
  Серийный номер:40:00:00:00:13:9E:D5:57:4F:E1:B3:23:01:17:0A:D0
 Идентификатор Закрытого ключа:
  Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
  Идентификатор Закрытого ключа: 8083SIC3XX01
 Ключ выработан в Центре Регистрации:
 X509v3 Область Применения Ключа:
  Электронная Подпись
  Неотрекаемый
  Шифрование Ключа
  Шифрование Данных
 X509v3 Срок Действия Закрытого Ключа:
  Действителен с:20 Июн 2012 11:25:32 GMT
  Действителен по:20 Сен 2013 23:59:00 GMT
 Средства ЭП и УЦ Издателя:
  Средство электронной подписи:
  СКЗИ Верба-OW (версия 6.1.2)
  Средство УЦ:
  Удостоверяющий центр АПК Верба-сертификат МВ версия 2.0
  Заключение на средство ЭП: СФ/124-1499 от 30.04 2010г.
  Заключение на средство УЦ: СФ/128-1500 от 22.06 2010г.
 X509v3 Основные Ограничения: критичное
  CA:FALSE
 X509v3 Политики Сертификата:
  Идентификатор Политики: 1.2.643.100.113.2 - класс средств ЭП КС2
 X509v3 Идентификатор Ключа Издателя:
  Идентификатор ключа:A3:3D:71:4F:F5:6E:6D:51:47:B6:6A:86:E9:A2:94:14:85:1F:86:88
  Имя в директории:OGRN=1234567890123/INN=123456789012/Email=mopniei@mo.msk..ru/C=ru/L=г.
 Москва/ST=77 Москва/streetAddress=ул.Сущёвский Вал д.16 стр.5 этаж 2/O=МО ПНИЭИ/CN=УЦ
 ЗАО МО ПНИЭИ
  Серийный номер:40:00:00:00:54:B2:43:81:4F:E1:AE:19:01:03:5A:A7

Алгоритм ЭП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
 FA:A7:E2:AE:8E:A6:9B:36:CD:14:C2:09:78:49:EC:73:
 70:D1:A2:01:5B:20:1B:F6:F3:49:0F:6F:C2:15:11:DE:
 CD:B7:E2:36:D7:67:94:3D:33:B3:FD:D2:D1:3A:2D:50:
```

Инфраструктура открытых ключей VCERT MV

74:65:18:21:E8:1A:F6:8B:6E:5F:E3:4B:63:72:4B:C0

Уполномоченное лицо

_____"____"_____**201__г.**

М.П.

Полномочный представитель организации:
(владелец сертификата ключа электронной подписи)

_____"____"_____**201__г.**

Приложение № 5 к Регламенту
Форма заявления на аннулирование
сертификата ключа проверки
электронной подписи для юридического лица

ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ (ОТЗЫВ) СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ.

(для юридического лица)

_____
(наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

в связи с _____

(причина аннулирования (отзыва) сертификата ключа проверки электронной подписи: компрометация) ключа электронной подписи, прекращение работы и т.д.)

просит аннулировать (отозвать) сертификат ключа проверки электронной подписи серийный номер _____, выданный на имя

_____
(фамилия, имя, отчество)

Владелец сертификата ключа подписи _____
(Фамилия И.О.)

_____«____» _____ 20____ г.

_____
(Должность и Фамилия И.О. уполномоченного лица организации)

_____
(Подпись уполномоченного лица организации, дата подписания заявления)

Печать организации)

Настоящим подтверждаю, что Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи подписи _____ (Ф.И.О.) получено.

«__» _____ 20__г.

Руководитель Удостоверяющего центра
ЗАО «МО ПНИЭИ» _____

Приложение №6 к Регламенту

Форма заявления на аннулирование
сертификата ключа проверки
электронной подписи для
физического лица, индивидуального предпринимателя

ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ (ОТЗЫВ) СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ .

(для физического лица, индивидуального предпринимателя)

От

ФИО_____

Паспорт №_____Серия_____

Выдан_____

СНИЛС_____

*ОГРНИП_____

_* Для индивидуального предпринимателя

в связи с _____

(причина аннулирования (отзыва) сертификата ключа проверки электронной подписи: компрометация) ключа электронной подписи, прекращение работы и т.д.)

прошу аннулировать (отозвать) сертификат ключа проверки электронной подписи серийный номер _____,

Владелец сертификата ключа подписи _____

(Фамилия И.О.)

_____«____» _____ 20____ г.

Настоящим подтверждаю, что Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи подписи _____ (Ф.И.О.) получено.

«__» _____ 20__г.

Руководитель Удостоверяющего центра

ЗАО «МО ПНИЭИ» _____

.