«Утверждаю»

Генеральный директор

ЗАО «Роста»

_____ /Кузнецов В.Б./

«…….»…….2008 г.

РЕГЛАМЕНТ
Удостоверяющего центра.

Ростов-на-Дону
2008

СОДЕРЖАНИЕ.

1. Сведения об Удостоверяющем Центре

«Удостоверяющий Центр ЗАО «Роста», является структурным подразделением ЗАО «Роста».

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

1. ЛИЦЕНЗИЯ Б 295164
Регистрационный № 825 Р от 24 июля 2006 г.
Управления ФСБ России по Ростовской области на деятельность по распространению шифровальных (криптографических) средств.

2. ЛИЦЕНЗИЯ Б 295016
Регистрационный № 698 от 25 августа 2005 г.
Управления ФСБ России по Ростовской области на деятельность по предоставлению услуг в области шифрования информации.

3. ЛИЦЕНЗИЯ Б 295165
Регистрационный № 826 Х от 24 июля 2006 г.
Управления ФСБ России по Ростовской области на деятельность по техническому обслуживанию шифровальных (криптографических) средств.

4. ЛИЦЕНЗИЯ № 46122
Федеральной службы по надзору в сфере связи на услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации.

5. ЛИЦЕНЗИЯ № 46121
Федеральной службы по надзору в сфере связи на телематические услуги связи.

6. ЛИЦЕНЗИЯ № 001451
Регистрационный № 0298 от 11 сентября 2006 г.
Федеральной службы по техническому и экспортному контролю на деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

7. ЛИЦЕНЗИЯ № 001498
Регистрационный № 0519 от 11 сентября 2006 г.
Федеральной службы по техническому и экспортному контролю на деятельность технической защите конфиденциальной информации.

2. Термины и определения.

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

Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу ключа и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
Закрытый ключ электронной цифровой подписи действует на определенный момент времени (действующий закрытый ключ) если:

- наступил момент времени начала действия закрытого ключа;
- срок действия закрытого ключа не истек;
- сертификат ключа подписи, соответствующий данному закрытому ключу не аннулирован (отозван);

Сертификат ключа электронной цифровой подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Копия сертификата ключа электронной цифровой подписи – документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный собственноручной подписью уполномоченного лица Удостоверяющего центра и печатью ЗАО «Роста».

Владелец сертификата ключа электронной цифровой подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Список отозванных сертификатов (СОС) – электронный документ с электронной цифровой подписью уполномоченного лица 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 электронной цифровой 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.

Удостоверяющий центр - юридическое лицо или его подразделение, выполняющее функции по изготовлению сертификатов ключей подписей для использования в информационных системах общего пользования, предусмотренные Федеральным законом об электронной цифровой подписи N 1-ФЗ от 10 января 2002 года.

Пользователь УЦ – физическое лицо, зарегистрированное в Удостоверяющем Центре и являющееся владельцем сертификата ключа подписи.

Псевдоним – вымышленное имя физического лица, которое он сознательно и легально принимает для регистрации в Удостоверяющем Центре.

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.

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 ключа электронной цифровой подписи;
- реестр заявлений на аннулирование (отзыв) сертификата ключа электронной цифровой подписи;
- реестр сертификатов ключей электронной цифровой подписи;
- реестр изготовленных списков отозванных сертификатов ключей электронной цифровой подписи;
- служебные документы Удостоверяющего центра.

Система защищенного электронного документооборота (ЭДО) – информационная система, представляющая собой совокупность программного обеспечения, обслуживаемого пользователями системы ЭДО и Удостоверяющим центром, а также вычислительных средств и баз данных, принадлежащих или подконтрольных пользователям системы защищенного ЭДО, предназначенная для передачи зашифрованных и подписанных ЭЦП электронных документов в целях обеспечения функционирования Электронного документооборота по правилам, установленным законодательством Российской Федерации и частными соглашениями между участниками системы ЭДО.

Пользователь Системы защищенного ЭДО – физическое лицо, или физическое лицо, уполномоченное юридическим лицом, подписавшее **Договор о предоставле-**

нии услуг УЦ ЗАО «Роста» или иной документ, определяющий его взаимоотношения с Удостоверяющим центром, и зарегистрированное в Удостоверяющем центре.

Средство электронной цифровой подписи и шифрования – средство криптографической защиты информации (СКЗИ) "Верба-OW" (версия 6.1) в составе согласно формуляру ЯЦИТ.00020-03 30 01 (вариант комплектации 3)

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 Договора 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 и шифрования.

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 Системы защищенного ЭДО, присоединившемуся к Регламенту в порядке, предусмотренном статьёй 428 ГК РФ, услуг по изготовлению и выдаче сертификатов ключей электронной цифровой подписи и дополнительных услуг, связанных с управлением сертификатами ключей подписи и шифрования, 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 «Роста» http://www.rosta.rostov.ru, либо в офисе Удостоверяющего Центра по адресу г. Ростов-на-Дону, пр. Ворошиловский, д. 52, оф. 67, и по запросу получить его копию за плату, не превышающую расходов на ее изготовление.

3.1.4 Присоединение к Регламенту производится путем заключения Пользователем Системы защищенного ЭДО Договор о **предоставлении услуг УЦ ЗАО «Роста»** (далее по тексту Договора), указанного в Приложении № 1 к Регламенту.

3.1.5 После присоединения в установленном порядке Пользователя Системы ЭДО к Регламенту, Стороны вступают в соответствующие договорные отношения на неопределённый срок.

3.1.6 Пользователь Системы ЭДО имеет право в одностороннем порядке без обращения в суд расторгнуть Договор, письменно уведомив об этом ЗАО «Роста» за один месяц до дня расторжения. Уведомление о расторжении Договора, полученное ЗАО «Роста» от Пользователя Системы ЭДО, является основанием для обязательного аннулирования сертификатов ключей подписей Пользователей УЦ, уполномоченных данным Пользователем Системы ЭДО. Датой аннулирования указанных сертификатов ключей Пользователей УЦ будет дата расторжения Договора. При этом Стороны до дня прекращения действия Договора обязаны разрешить между собой все денежные и иные имущественные вопросы, связанные с Договором.

3.1.7 Расторжение Договора 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 (863) 242-51-37.

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 Системы ЭДО.

3.3.2 Уведомление Пользователя Системы ЭДО о внесении изменений (дополнений) в Регламент осуществляется путем размещения указанных изменений (дополнений) на сайте ЗАО «Роста» http://www.rosta.rostov.ru.

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 «Роста» http://www.rosta.rostov.ru.

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 Системы защищенного ЭДО, 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 электронной цифровой подписи Пользователей УЦ в электронной форме.

3.4.3 Изготовление копий сертификатов ключей электронной цифровой подписи Пользователей УЦ на бумажном носителе.

3.4.4 Ведение реестра изготовленных сертификатов ключей электронной цифровой подписи Пользователей УЦ.

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

3.4.6 Аннулирование (отзыв) сертификатов ключей электронной цифровой подписи по обращениям Владельцев сертификатов ключей электронной цифровой подписи.

3.4.7 Предоставление Пользователям УЦ сведений об аннулированных сертификатах ключей электронной цифровой подписи и шифрования.

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

3.4.9 Подтверждение подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах ключей подписи и шифрования по обращениям Пользователей УЦ.

4. Права и обязанности сторон.

4.1. Удостоверяющий центр имеет право:

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

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

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

4.2. Пользователь УЦ имеет право:

– получить список отозванных сертификатов ключей электронной цифровой подписи, изготовленный Удостоверяющим центром;

– применять сертификат ключа электронной цифровой подписи Уполномоченного лица Удостоверяющего Центра для проверки электронной цифровой подписи уполномоченного лица Удостоверяющего центра в сертификатах ключа электронной цифровой подписи, изготовленных Удостоверяющим центром;

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

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

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

– обратиться в Удостоверяющий центр за подтверждением подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего Центра в изготовленных им сертификатах ключей электронной цифровой подписи;

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

4.3. Обязанности Удостоверяющего центра.

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

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

4.3.3 Удостоверяющий центр обязан принять меры по защите закрытого ключа Уполномоченного лица 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 электронной цифровой подписи.

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

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

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

Удостоверяющий центр обязан:

- Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей электронной цифровой подписи Пользователей УЦ;
- Обеспечить уникальность значений открытых ключей в изготовленных сертификатах ключей электронной цифровой подписи Пользователей УЦ.

4.3.9 Удостоверяющий центр обязан аннулировать (отозвать) сертификат ключа электронной цифровой подписи по заявлению на аннулирование (отзыв) сертификата ключа электронной цифровой 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 электронной цифровой подписи по адресу http://www.rosta.rostov.ru/certifying_center/vcert_mv/CN=RostaCA,O=Rosta,C=ru.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 цифровой подписи и шифрования.

4.4.1 Владелец сертификата ключа электронной цифровой подписи обязан хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

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

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

4.4.4 Владелец сертификата ключа электронной цифровой подписи обязан немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) сертификата ключа электронной цифровой подписи 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.

4.4.5 Владелец сертификата ключа электронной цифровой подписи обязан не использовать личный закрытый ключ, связанный с сертификатом ключа электронной цифровой 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 электронной цифровой подписи обязан не использовать личный закрытый ключ, связанный с аннулированным (отозванным) сертификатом ключа электронной цифровой 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 «Роста» 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 «Роста» несет ответственность за убытки при использовании закрытого ключа и сертификата ключа электронной цифровой подписи Пользователя УЦ, только в случае если данные убытки возникли при компрометации закрытого ключа уполномоченного лица Удостоверяющего Центра, либо вследствие несоответствий сведений в сертификате ключа электронной цифровой 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 Системы ЭДО.

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 «Роста» и Пользователь Системы защищенного ЭДО

6.2 Все споры и разногласия между Сторонами, возникающие из Регламента или в связи с ним, в том числе касающиеся заключения, действия, исполнения, изменения, прекращения Договора о предоставлении услуг УЦ по которым не было достигнуто соглашение, разрешаются в Арбитражном суде города Ростова-на-Дону.

7 Порядок пользования услугами Удостоверяющего Центра.

7.1 Пользователь Системы защищенного ЭДО подписывает Договор о предоставлении услуг УЦ ЗАО «Роста» (Приложение № 1).

7.2 Лицо, уполномоченное Пользователем Системы защищенного ЭДО, предоставляет в Удостоверяющий центр или в организацию - партнер ЗАО «Роста», исполняющую функции Центра Регистрации, доверенность на осуществление процедуры регистрации для получения сертификата ключа электронной цифровой подписи (приложение №3) и заявление о регистрации в реестре Пользователей Удостоверяющего центра ЗАО «Роста» на имя его руководителя (Приложение № 2).

7.3 Уполномоченное лицо Удостоверяющего центра или лицо, уполномоченное организацией - партнером ЗАО «Роста» и действующее от его имени на основании Договора поручения проводит (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 «Роста» или организация - партнер ЗАО «Роста», исполняющая функции Центра Регистрации, выставляет счет на оплату услуг в соответствии с Договором.

7.5 После оплаты Пользователем выставленного счета, Администратор Центра Регистрации на основании полноты и достаточности предоставленных документов производит регистрацию пользователя в системе;

7.6 Используя ПО Центр Регистрации, администратор формирует ключ и лицензию регистрации пользователя. В лицензию регистрации пользователя заносятся дополнения, необходимые для обеспечения функционирования прикладной системы и системы управления ключами. При наличии почтового адреса ЦР в сертификат заносится дополнение **Альтернативное Имя Издателя** с указанием почтового адреса ЦР в поле rfc822Name. При наличии почтового адреса пользователя в сертификат заносится дополнение **Альтернативное Имя Владельца** с указанием почтового адреса пользователя в поле rfc822Name. В лицензии регистрации устанавливается дополнение **Регламент регистрации**. В лицензию регистрации записываются сертификаты ЦС, ЦР и СОС ЦС и СОЛ ЦР. При формировании имени Владельца сертификата Центр Регистрации обеспечивает уникальность имени пользователя в системе;

7.7 Бланк лицензии регистрации пользователя выводится на принтер в двух экземплярах и заверяется администратором ЦР и пользователем. Один экземпляр бланка лицензии регистрации хранится у администратора ЦР, второй экземпляр – у пользователя;

7.8 Администратор ЦР выдает пользователю карточку оповещения о компрометации, в которой отражаются телефоны и пароли УЦ и пользователя (Рисунок 1. Карточка оповещения о компрометации.);

В Карточке оповещения указаны: телефоны УЦ, пароль (кодовое слово) УЦ, уникальный пароль (кодовое слово), присвоенный пользователю УЦ.

Примечание. Карточка оповещения используется участниками системы для сообщений о компрометации ключа по телефонным каналам общего пользования. Карточка оповещения должна храниться у пользователя наравне с ключами.

Пароль УЦ	Основной пароль	Резервный пароль
Телефоны Администратора ЦР		
Пароль пользователя	Основной пароль	Резервный пароль

Рисунок 1. Карточка оповещения о компрометации

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

7,10 Администратор ЦР делает запись в «Журнале регистрации пользователей Удостоверяющего центра» (Приложение № 7).

Примечание. При регистрации каждого пользователя системы администратор ЦР передает пользователю копию бланка сертификата ЦС и сертификата ЦР.

7.11 Ключ и лицензия регистрации пользователя

При формировании секретного ключа (ключа регистрации) и сертификата (лицензии регистрации) пользователя предлагается использовать следующие значения.

- срок действия секретного ключа пользователя– 1 год 3 месяца;
- срок действия сертификата пользователя – 5 лет;
- срок действия ключа регистрации пользователя – 1 месяц;

Имя владельца сертификата пользователя может иметь следующий вид:

Поле	**Значение**	**Примечание**
C	RU	страна (country)
O	PKI	организация (organization)
ST	Moscow region	область (StateOrProvance) Moscow
L	Moscow	Место нахождения (locality)
OU	ACME	подразделение (organizationUnit)
CN	Name	имя (commonName)

В результате регистрации Пользователь получает:

- ключ регистрации;
- Лицензию регистрации, содержащую сертификаты Уполномоченного лица Удостоверяющего Центра (Центра Сертификации (ЦС), Центра Регистрации (ЦР) и действующие списки отозванных сертификатов (СОС);
- заверенный бланк лицензии регистрации Пользователя УЦ (2 экз.);
- копии бланков сертификатов ЦС и ЦР;

Пользователь со своей стороны заверяет бланк лицензии регистрации. Один экземпляр бланка лицензии регистрации хранится у Пользователя, второй - передается в Удостоверяющий Центр (или организацию - партнер ЗАО «Роста», исполняющую функции Центра Регистрации). Лицензия регистрации является лицензией на формирование ключевой информации Пользователем.

7.12 Формирование ключей Пользователем

7.12.1 Пользователь формирует собственные секретный и открытый ключи ЭЦП, формирует запрос на выпуск соответствующего сертификата и передает запрос на сертификат в Удостоверяющий Центр (или его партнерам).

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 добавляются сертификат УЦ (Сертификат уполномоченного лица ЦС). Сертификат ЦР. Лицензия регистрации Пользователя и СОС добавляются в локальный справочник Пользователя. ПСП защищается с использованием ключа регистрации Пользователя;
- пользователь производит формирование личного секретного ключа ЭЦП и запроса на сертификат, содержащего открытый ключ ЭЦП Пользователя. С секретного ключа Пользователя формируется резервная копия, которая хранится у администратора безопасности (при его наличии) или у ответственного лица. Пометка о формировании ключа и запроса на сертификат заносится в «Журнал пользователя УЦ» (Приложение №8);
- формирование нового секретного и открытого ключа (ключей) 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 ЭЦП запроса на сертификат производится на вновь изготовленном секретном ключе Пользователя;
- запрос на сертификат в электронной форме передается в Центр Регистрации с использованием электронной почты. При этом запрос записывается и передается в формате упакованных данных (PKCS#7 Signed с использованием ключа и сертификата регистрации или действующего ключа 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)

7.12.2 Бланк запроса на сертификат (Приложение №6) выводится на принтер в двух экземплярах и заверяется пользователем, (администратором безопасности при его наличии) и ответственными лицами организации (директором и главным бухгалтером).

7.12.3 При наличии сетевого взаимодействия организации с ЦР, а так же наличии ПО на АРМ пользователя, поддерживающего обмен электронной почтой по протоколу SMTP, запрос на сертификат может быть передан в Центр Регистрации с использованием электронной почты. При этом запрос записывается и передается в формате упакованных данных с использованием ЭЦП на ключе регистрации пользователя (или действующем секретном ключе).

7.12.4 При отсутствии сетевого взаимодействия организации с ЦР, запрос записывается на магнитный носитель (дискету) в формате упакованных данных с ис-

пользованием ЭЦП на ключе регистрации пользователя (или действующем секретном ключе).

7.12.5 Если запрос на сертификат был передан по электронной почте, пользователь (администратор безопасности) должны передать обе копии бланка запроса в Центр Регистрации, используя для этого доступные способы доставки (например, заказное письмо).

7.12.6 Если запрос был записан на магнитный носитель, пользователь (администратор безопасности) прибывают в Центр Регистрации (ЦУКС) вместе с записанным запросом и заверенными бланками запроса;

7.12.7 При получении запроса на сертификат администратор ЦР 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 секретных ключей пользователя;
- может изменить срок действия сертификата пользователя;
- может изменить поля дополнения **Альтернативное Имя Владельца**, за исключением тех, которые не 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;

7.12.8 Администратор ЦР передает сформированный "шаблон" сертификата администратору ЦС. Администратор ЦС произведя верификацию "шаблона" (проверив ЭЦП ЦР), формирует сертификат пользователя. Сертификат пользователя хранится в базе ЦС в течение установленного срока хранения (равного сроку действия сертификата);

7.12.9 Администратор ЦС выводит на принтер две копии бланка сертификата пользователя (Приложение №4)и делает запись о формировании сертификата в "Журнале пользователя системы ЭДО;

7.12.10 Сертификат пользователя вместе с бланками передается администратору ЦР.

7.12.11 Удостоверяющий Центр обязан подготовить личный сертификат Пользователя в течение 2 (двух) рабочих дней с момента получения запроса

Получение личного сертификата пользователем

Личный сертификат может быть получен следующими способами:

– при личном присутствии пользователя (администратора безопасности) в Центре Регистрации;

– по электронной почте, если запрос на сертификат пользователя был получен ЦР по почте, и в сертификате пользователя есть зарегистрированный адрес электронной почты.

В любом из перечисленных случаев сертификат не передается пользователю до тех пор, пока Центр Регистрации не получит заверенный бланк запроса на сертификат.

При передаче личного сертификата пользователю ему так же передается заверенный Центром Регистрации бланк запроса и сертификата пользователя. Вторые копии этих бланков хранятся в Центре Регистрации.

При наличии сетевого справочника LDAP, администратор ЦР с использованием специализированного ПО администрирования справочника, производит публикацию сертификата пользователя.

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

7.13 . Повторная регистрация пользователя.

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

7.14 Обновление сертификата Пользователя

Обновление сертификата Пользователя может быть вызвано следующими причинами:

- окончанием срока действия секретного ключа;
- окончанием срока действия сертификата.

Формирование нового секретного ключа, запроса на сертификат, передача запроса в ЦР и получение сертификата производится согласно последовательности, описанной в п.п. 7.12.1 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.

7.15 Плановая смена ключей Пользователя УЦ .

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

Формирование нового секретного ключа, запроса на сертификат, передача запроса в ЦР и получение сертификата производится согласно последовательности, описанной в п.п. 7.12.1 настоящего Регламента, за исключением необходимости формирования ПСП Пользователя.

7.16 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 ЦР о компрометации ключей Пользователя.

Информация о компрометации может передаваться в ЦР по телефону с сообщением заранее условленного пароля, зарегистрированного в "Карточке оповещения о компрометации".

При наличии сетевого взаимодействия пользователь может оповестить ЦР путем формирования электронного сообщения о компрометации с использованием ПО «Справочник сертификатов» и передачей его в ЦР.

После компрометации ключей Пользователь формирует новый секретный ключ и запрос на сертификат. Так как Пользователь не может использовать скомпрометированный ключ для формирования ЭЦП и передачи запроса в защищенном виде по сети, запрос на сертификат (на магнитом носителе) вместе с заверенными бланками запроса доставляется лично или через специальную почтовую связь Пользователем (администратором безопасности) в Центр Регистрации.

7.17 Действия ЦР при компрометации ключей Пользователя.

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

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

При наличии сетевых средств распространения СОС, администратор ЦР производит публикацию СОС.

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

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

7.18 Исключение Пользователя УЦ из Удостоверяющего центра.

Исключение Пользователя из УЦ может быть осуществлено на основании письменного заявления Пользователя УЦ в адрес руководителя Удостоверяющего Центра, (Приложение №5) заверенного руководством Пользователя системы защищенного ЭДО Исключение Пользователя из УЦ аналогично компрометации ключа Пользователя. Получив такое заявление, администратор ЦР производит действия, описанные в п.7.16, 7,17.

7.19 Порядок разбора конфликтных ситуаций, связанных с применением ЭЦП.

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

Разбор подобных конфликтных ситуаций в соответствии с действующим законодательством и особенностями формирования самой электронной цифровой под-

писи требует применения специального программного обеспечения для выполнения проверок и документирования данных, используемых при выполнении процедуры проверки соответствия ЭЦП содержимому электронного документа.

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

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

При проверке значения ЭЦП используется открытый ключ, значение которого вычисляется по значению секретного ключа ЭЦП при их формировании.

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

Разбор конфликтной ситуации выполняется комиссией, состоящей из представителей сторон, службы безопасности и экспертов. Состав комиссии, порядок ее формирования, регламент работы, рассмотрение результатов определяется в приложении к Регламенту системы (Договору), заключаемому между участниками автоматизированной системы.

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

7.19.1 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** для электронного документа, авторство или содержание которого оспаривается.

Протокол проверки ЭЦП, 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 ЭЦП;
- проверка ЭЦП электронного документа с использованием сертификата;
- определение даты формирования каждой ЭЦП в электронном документе;
- проверка ЭЦП сертификата;
- проверка действительности сертификата на текущий момент времени;
- проверка действительности сертификата на момент формирования ЭЦП;
- проверка отсутствия сертификата в СОС.

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

При необходимости комиссия определяет правомерность использования сертификата на конкретном этапе технологического цикла системы банковских расчетов, опираясь на дополнения **Регламенты использования сертификата** и **Расширенные области использования ключа**, зарегистрированные для этого сертификата. Для этого комиссии дополнительно должны быть представлены подтверждения использования данных дополнений в прикладном программном обеспечении.

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

Примечание. Несовпадение даты формирования документа и сроков действия сертификата и/или сроков действия секретного ключа **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.

7.19.2 Случаи невозможности проверки значения ЭЦП

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

8. Дополнительные положения.

8.1 Плановая смена ключей Центра Сертификации УЦ.

За два месяца до окончания срока действия секретного ключа уполномоченного лица УЦ администратор УЦ производит формирование нового секретного ключа и сертификата уполномоченного лица УЦ (ЦС).

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

При переходе ЦС на вновь изготовленный ключ (сертификат), ЦС формирует СОС с использованием нового ключа.

Администратор ЦР публикует новый сертификат ЦС (в формате упакованных данных с использованием ЭЦП на действующем ключе ЦС) по адресу:
http://www.rosta.rostov.ru/certifying_center/vcert_mv/CN=RostaCA,O=Rosta,C=ru.cer

Все Пользователи системы во время, оставшееся до окончания срока действия секретного ключа УЦ, обязаны получить новый сертификат УЦ и добавить его в

ПСП с использованием ПО «Справочник сертификатов» без удаления действующего сертификата ЦС.

8.2 Плановая смена ключей Центра Регистрации УЦ.

За два месяца до окончания срока действия секретного ключа ЦР администратор ЦР производит формирование нового секретного ключа и сертификата ЦР.

Смена ключей Центра Регистрации производится аналогично смене ключей Пользователя.

Все Пользователи системы во время, оставшееся до окончания срока действия секретного ключа ЦР, обязаны получить новый сертификат ЦР.

8.3 Компрометация ключей Центра сертификации и Центра Регистрации.

8.3.1 По факту компрометации ключей должно быть проведено служебное расследование. Выведенные из действия, скомпрометированные ключевые носители после проведения служебного расследования уничтожаются, о чем делается запись в "Журнале пользователя системы ЭДО".

8.3.2 Компрометация ключей Центра Сертификации

В случае компрометации ключа Центра Сертификации 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 СОС ЦС, с указанием в нем отзываемого сертификата ЦС;
- обеспечить получение сертификата и СОС ЦС всеми пользователями системы;
- произвести выпуск новых сертификатов всех пользователей, используя действующие сертификаты;
- обеспечить получение новых личных сертификатов пользователями системы.

8.3.3 Компрометация ключей Центра Регистрации

Компрометация ключа ЦР не приводит к остановке системы. В случае компрометации становится невозможным сетевое взаимодействие между пользователем системы и ЦР в части управления ключевой системой.

В случае компрометации ключа Центра Регистрации должны быть выполнены следующие мероприятия:

- ЦС формирует СОС, с указанием в нем отзываемого сертификата ЦР;
- 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 СОС (приложение № 4 к настоящему Регламенту) обеспечивается Центром Сертификации. Период обновления СОС составляет 300 дней.

При этом Удостоверяющий центр обеспечивает публикацию СОС по адресу: http://www.rosta.rostov.ru/certifying_center/vcert_mv/CN=RostaCA,O=Rosta,C=ru.crl

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

Для распространения вновь изданного СОС, 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 СОС, хранящийся в локальном справочнике сертификатов с использованием ПО «Справочник сертификатов».

8.5 Хранение сертификатов ключа подписи и шифрования в Удостоверяющем Центре.

Срок хранения сертификата ключа подписи и шифрования в Удостоверяющем Центре осуществляется в течение всего периода его действия и 5 (Пять) лет после его аннулирования (отзыва). По истечении указанного срока хранения сертификаты ключа подписи и шифрования 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 открытых ключей уполномоченного лица Удостоверяющего Центра;
- аннулированные сертификаты пользователей Удостоверяющего Центра;
- заявления на регистрацию пользователей в Удостоверяющем Центре;
- запросы на сертификат ключа подписи и шифрования;
- заявления на аннулирование (отзыв) сертификатов открытых ключей;
- служебные документы Удостоверяющего Центра.

Документы Удостоверяющего Центра на бумажных носителях, в том числе и сертификаты ключа подписи и шифрования 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 цифровой подписи и списков отозванных сертификатов.

Удостоверяющий центр издает сертификаты открытых ключей Пользователей УЦ в электронной форме формата X.509 версии 3 и список отозванных сертификатов (СОС) в электронной форме формата X.509 версии 2.

- **Структура сертификата ЦС**

Данные Сертификата:
Версия: 3 (0x2)
Серийный Номер:40:00:00:00:3F:0E:1C:2B:48:3A:BE:80:0A:7C:24:71
Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
Издатель: CN=Rosta CA,O=Rosta,C=ru
Срок действия
Действителен с: 26 Май 2008 13:40:00 GMT
Действителен по: 26 Май 2013 23:59:00 GMT
Владелец: CN=Rosta CA,O=Rosta,C=ru
Открытый Ключ Владельца:
Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
Открытый ключ ГОСТ 34.11-2001:
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
06:F1:FF:86:DA:8F:D4:EE:C3:D7:4E:6A:E3:F8:EB:82:
27:17:D8:D8:C5:92:61:13:0B:C0:19:79:CF:23:94:87:
F8:38:D2:67:A2:E5:8C:D3:BC:48:60:6B:E0:16:86:73:
07:38:8F:85:18:CA:60:93:DA:3B:3F:37:72:37:8F:46
Дополнения X.509:
X509v3 Альтернативное Имя Владельца:
URI:www.rosta.rostov.ru
Организация:ЗАО "Роста"
Зарегистрированный Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф
.67
Должность:Уполномоченное лицо ЦС
Номер Телефона:(863)2263104
Почтовый Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф.67

X509v3 Срок Действия Закрытого Ключа:
Действителен с:26 Май 2008 13:40:00 GMT
Действителен по:26 Авг 2009 23:59:00 GMT

Идентификатор Закрытого ключа:
Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
Идентификатор Закрытого ключа: 2702TOE1W401

X509v3 Идентификатор Ключа Владельца:
67:EF:80:E7:A2:73:0B:B9:7F:6A:FD:B9:DE:BE:77:34:42:38:54:FB

X509v3 Основные Ограничения:
CA:TRUE

X509v3 Область Применения Ключа:
Электронная Подпись
Подпись Сертификата
Подпись COC

X509v3 Точка Распространения COC:
URI:http://www.rosta.rostov.ru/certifying_center/vcert_mv/CN=RostaCA,O=Rosta,
C=ru.crl

Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
81:EE:F7:B2:EA:E9:71:9E:16:BC:75:A5:0F:E6:62:A5:
06:C5:72:2F:15:BD:B7:AD:C6:28:27:75:11:65:B4:10:
A6:C0:AB:4B:ED:05:90:BF:C2:D4:C4:A6:69:0A:79:57:
25:A7:93:D7:5D:DB:C7:4F:64:E2:AD:7D:55:09:9D:4F

- **Структура COC**

Список Отозванных Сертификатов (CRL):
Данные:
Версия 2 (0x1)
Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
Издатель: CN=Rosta CA,O=Rosta,C=ru
Дата Выпуска: 28 Май 2008 13:23:26 GMT
Следующий Выпуск: 28 Май 2009 13:23:26 GMT
Дополнения X.509 COC:
X509v3 Номер Списка Отзыва:
3

X509v3 Точка Распространения COC:
URI:http://www.rosta.rostov.ru/certifying_center/vcert_mv/CN=RostaCA,O=Rosta
,C=ru.crl
RelativeName:<UNSUPPORTED>

X509v3 Идентификатор Ключа Издателя:
keyid:67:EF:80:E7:A2:73:0B:B9:7F:6A:FD:B9:DE:BE:77:34:42:38:54:FB
Имя в директории:C=ru/O=Rosta/CN=Rosta CA
Серийный номер:40:00:00:00:3F:0E:1C:2B:48:3A:BE:80:0A:7C:24:71

Отозванные Сертификаты: Отсутствуют Отозванные Сертификаты.
Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
D0:6E:E8:65:61:89:B0:9B:4D:03:13:48:4E:03:50:85:
77:B4:9E:11:83:35:55:B2:89:B9:45:DB:4B:9F:1A:C3:
F1:42:DB:76:37:1C:58:DE:B4:B0:88:16:A8:47:A4:84:
9E:21:C4:69:35:5B:6D:DC:57:27:E9:E2:4A:98:A9:63

- **Структура сертификата пользователя**

Данные Сертификата:
Версия: 3 (0x2)
Серийный Номер:40:00:00:00:4D:D7:59:44:48:3D:6B:11:0B:55:51:EA
Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
Издатель: CN=Rosta CA,O=Rosta,C=ru
Срок действия
Действителен с: 28 Май 2008 14:24:19 GMT
Действителен по: 26 Май 2013 23:59:00 GMT
Владелец: CN=Lychagin,O=Rosta,C=ru
Открытый Ключ Владельца:
Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
Открытый ключ ГОСТ 34.11-2001:
Параметры алгоритма:
Параметры открытого ключа: Параметры Диффи-Хеллман вариант провайдера
Параметры хэширования: Узел замены для хэша вариант провайдера
длина ключа: 512 бит
01:94:D1:56:4E:D8:95:73:01:97:E7:23:87:97:06:41:
23:FB:E1:EE:57:50:C8:B3:CF:08:E2:D2:D2:D6:86:71:
57:77:E6:F4:87:EC:6C:43:CD:CA:63:A8:B7:52:73:3D:
96:5D:47:50:53:EE:C6:0D:DB:1F:BF:39:FF:79:AD:6A
Дополнения X.509:
X509v3 Основные Ограничения:
CA:FALSE

Ссылка на Сертификат Регистрации:
Имя в директории:C=ru/O=Rosta/CN=Rosta RA
Серийный номер:40:00:00:00:D0:09:05:7D:45:F7:BA:6A:01:7D:D9:0D

X509v3 Идентификатор Ключа Владельца:
27:FC:ED:33:DC:1B:32:EC:7F:23:80:A2:B5:0E:18:3E:10:E3:B9:B2

Ссылка на предыдущий сертификат:
keyid:CF:21:EA:2C:B9:5F:78:CA:54:00:D5:B3:FE:00:8A:0D:DB:09:D8:BF
Имя в директории:C=ru/O=Rosta/CN=Rosta CA
Серийный номер:40:00:00:00:33:CA:A7:0D:45:F7:BD:02:01:87:F9:85

Идентификатор Закрытого ключа:
Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
Идентификатор Закрытого ключа: 1113L4SRJE01

X509v3 Область Применения Ключа:
Электронная Подпись
Шифрование Ключа
Шифрование Данных

X509v3 Альтернативное Имя Владельца:
Почтовый адрес RFC822:rosta-support@aaanet.ru
URI:www.rosta.rostov.ru
Организация:ЗАО "Роста"

Зарегистрированный Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф .67
Фамилия:Лычагин Алексей Александрович
Должность:Администратор УЦ
Номер Телефона:(863)2994867, (863)2263104
Почтовый Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф.67

X509v3 Срок Действия Закрытого Ключа:
Действителен с:28 Май 2008 14:24:19 GMT
Действителен по:28 Авг 2009 23:59:00 GMT

X509v3 Расширенная Область Применения Ключа:
Защита эл. почты (1.3.6.1.5.5.7.3.4)

X509v3 Идентификатор Ключа Издателя:
keyid:67:EF:80:E7:A2:73:0B:B9:7F:6A:FD:B9:DE:BE:77:34:42:38:54:FB
Имя в директории:C=ru/O=Rosta/CN=Rosta CA
Серийный номер:40:00:00:00:3F:0E:1C:2B:48:3A:BE:80:0A:7C:24:71

X509v3 Точка Распространения COC:
URI:http://www.rosta.rostov.ru/certifying_center/vcert_mv/CN=RostaCA,O=Rosta, C=ru.crl

X509v3 Альтернативное Имя Издателя:
URI:www.rosta.rostov.ru
Организация:ЗАО "Роста"
Зарегистрированный Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф .67
Должность:Уполномоченное лицо ЦС
Номер Телефона:(863)2263104
Почтовый Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф.67

Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
A6:DC:AC:9A:B9:FD:E4:D0:FA:EB:DD:4C:39:B5:6F:02:
A7:A0:44:EB:F0:E8:4F:99:F4:6E:D4:B0:BA:C3:4D:CD:
F0:5B:A5:70:62:09:0C:6B:35:83:A9:9A:6B:07:FC:28:
D3:6B:A8:33:87:DE:66:8C:14:12:0E:28:26:BA:F8:E9

8.8 Установление доверительных отношений между УЦ ЗАО «Роста» и УЦ внешних организаций

Установление доверительных отношений между двумя УЦ является организационно-технической процедурой, в результате которой участники ЭДО, получившие сертификаты ключей подписи в одном УЦ, получают возможность проверить подлинность ЭЦП в ЭД участников ЭДО, получивших сертификаты в другом УЦ.

Для установления доверительных отношений каждая из Сторон (УЦ ЗАО «Роста» и УЦ внешней организации оформляет на бумажном носителе «Список сертификатов ключей подписи удостоверяющего центра», включающий сертификаты ключей подписи уполномоченных лиц УЦ и выпущенные кросс-сертификаты ключей подписи уполномоченных лиц доверенных УЦ, которыми будут заверяться ключи подписи пользователей, зарегистрированных в данном УЦ и в доверенных УЦ. К Списку прилагаются распечатанные на бумажных носителях соответствующие сертификаты ключей подписи, указанные в Списке.

Список подписывается начальником УЦ ЗАО «Роста» и руководителем УЦ внешней организации, скрепляется печатями УЦ ЗАО «Роста» и УЦ внешней организации, и передается под расписку другой Стороне.

Список отозванных сертификатов (СОС) и сертификаты ключей подписи Уполномоченных лиц УЦ внешней организации в электронном виде передаются в УЦ ЗАО «Роста», а сертификаты ключей подписи Уполномоченных лиц УЦ ЗАО «Роста» и СОС УЦ ЗАО «Роста» в электронном виде передаются в УЦ внешней организации.

В каждом из УЦ производится сравнение электронных сертификатов ключей подписи Уполномоченных лиц УЦ другой Стороны с распечатанными сертификатами на бумажных носителях и ввод их в действие. При этом сертификаты заверяются ЭЦП Уполномоченного лица соответствующего УЦ.

При любом изменении в Списке сертификатов ключей подписи Уполномоченных лиц УЦ соответствующая Сторона оформляет новый Список с приложенными Сертификатами уполномоченных лиц УЦ и передает его другой Стороне.

8.9 Порядок взаимодействия УЦ при формировании новых списков отозванных сертификатов, при смене ключей подписи Уполномоченных лиц УЦ.

При изменении СОС в случае отзыва или приостановки действия сертификатов ключей подписи пользователей УЦ новый СОС высылается в УЦ каждой из Сторон. Полученные СОС подписываются Уполномоченным лицом УЦ и размещаются в точках публикации УЦ.

Уполномоченные лица УЦ каждой из Сторон обязаны производить периодическую (плановую) замену своих ключей подписи не реже заданного срока действия ключа подписи. В целях обеспечения действительности сертификатов ключей подписи пользователей УЦ, заверенных подписью Уполномоченного лица соответствующего УЦ, замена ключей подписи Уполномоченного лица УЦ должна быть произведена до окончания его срока действия не менее чем за срок действия сертификатов пользователей УЦ.

В случае компрометации ключей подписи Уполномоченное лицо УЦ обязано:

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

После выполнения действий, производится оформление на бумажном носителе нового Списка сертификатов ключей подписи УЦ в соответствии с разделом 8.8 настоящего Регламента и передача новых сертификатов уполномоченного лица УЦ в электронном виде в УЦ другой Стороны;

Уполномоченное лицо УЦ осуществляет сравнение новых электронных сертификатов Уполномоченных лиц УЦ другой Стороны с сертификатами, распечатанными на бумажных носителях и вводит их в

9 Конфидециальность.

9.1 Типы конфиденциальной информации.

Закрытый ключ, соответствующий сертификату ключа подписи и шифрования Пользователя УЦ является конфиденциальной информацией данного Пользователя УЦ. Удостоверяющий Центр не осуществляет хранение закрытых ключей пользователей.

Персональная информация Пользователей УЦ и корпоративная информация Пользователей системы защищенного ЭДО, содержащаяся в Удостоверяющем Центре, не подлежащая непосредственной рассылке в качестве части сертификата ключа подписи и шифрования, 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 подписи и шифрования 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 «Роста» 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 «Роста» и Удостоверяющего центра осуществляется посредством применения электромеханических средств контроля доступа. Ключи (электронные ключи доступа) от помещения предоставлены сотрудникам Удостоверяющего центра по решению руководителя ЗАО «Роста».

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 «Роста» 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

Договор о предоставлении услуг Удостоверяющего Центра ЗАО «Роста»

г. Ростов-на-Дону *“ ” _____ 200__ г.*

ЗАО «Роста», в лице Генерального директора Кузнецова В. Б., действующего на основании Устава, с одной стороны, и
_____, именуемый в дальнейшем «Пользователь системы защищенного ЭДО», действующего на основании _____, с другой стороны, именуемые также Стороны, заключили настоящий Договор о нижеследующем.

СТАТЬЯ 1. ПРЕДМЕТ ДОГОВОРА

В силу настоящего Договора Пользователь системы защищенного ЭДО присоединяется к Регламенту Удостоверяющего центра ЗАО «Роста» (далее по тексту Регламенту).

Настоящий Договор определяет взаимные права и обязанности ЗАО «Роста», Удостоверяющего центра ЗАО «Роста» и Пользователя системы защищенного ЭДО в связи с осуществлением защищенного электронного документооборота в соответствии с Регламентом.

СТАТЬЯ 2. ОБЩИЕ ПОЛОЖЕНИЯ

ЗАО «Роста» и Пользователь системы защищенного ЭДО признают применение СКЗИ в соответствии с Регламентом достаточным для обеспечения конфиденциальности и целостности информации и невозможности ее фальсификации.

СТАТЬЯ 3. ПРАВА ЗАО «РОСТА» И УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.

Удостоверяющий центр ЗАО «Роста» осуществляет все права, вытекающие из Регламента, включая следующие:

- в одностороннем порядке вносить изменения, дополнения в Регламент, а также прекращать их действие;
- при возникновении в Системе защищенного электронного документооборота ситуаций, признаваемых чрезвычайными в соответствии с Регламентом, принимать меры, направленные на преодоление чрезвычайных ситуаций, а также требовать от Пользователя системы защищенного ЭДО совершения действий или воздержания от совершения действий в связи с осуществлением мер, предпринимаемых в соответствии с Регламентом для преодоления чрезвычайных ситуаций.

ЗАО «Роста» вправе:

- определять размер и порядок осуществления оплаты за услуги Удостоверяющего центра по изготовлению криптографических ключей и сертификатов ключей электронной подписи;
- в одностороннем порядке расторгать Договор в случае неисполнения или ненадлежащего исполнения Пользователем системы защищенного ЭДО обязанностей, предусмотренных настоящим Договором и Регламентом, включая нарушение Пользователем системы защищенного ЭДО установленного Регламентом порядка разрешения конфликтных ситуаций и споров;
- осуществлять иные права, возникающие в соответствии с Регламентом.

СТАТЬЯ 4. ОБЯЗАННОСТИ ЗАО «РОСТА» И УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.

Удостоверяющий центр обязуется исполнять Регламент, в том числе своевременно и в полном объеме выполнять следующие обязанности:

- своевременно извещать Пользователя системы защищенного ЭДО об изменениях и дополнениях, вносимых в Регламент или прекращении их действия;
- организовывать работу с криптографическими ключами Пользователя системы защищенного ЭДО в объеме и в соответствии с порядком, определяемым Регламентом и Приложениями к нему.

ЗАО «Роста» обязуется:

- соблюдать режим конфиденциальности информации, касающейся паролей, идентификаторов, а также криптографических ключей, которая становится доступной Удостоверяющему центру в связи с выполнением им своих функций в соответствии с Регламентом;
- выполнять иные обязанности перед, Пользователем системы защищенного ЭДО, возникающие в соответствии с Регламентом.

СТАТЬЯ 5. ПРАВА ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ ЗАЩИЩЕННОГО ЭДО.

Пользователь системы защищенного ЭДО в соответствии с Регламентом осуществляет следующие права:

- требовать от Удостоверяющего центра организации работы с криптографическими ключами Пользователя системы защищенного ЭДО в объеме и в соответствии с порядком, определяемым Регламентом и Приложениями к нему;
- осуществлять иные права, возникающие в соответствии с Регламентом.

СТАТЬЯ 6. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ ЗАЩИЩЕННОГО ЭДО.

Пользователь системы защищенного ЭДО обязуется исполнять Регламент, изменения и дополнения к нему, в том числе своевременно и в полном объеме выполнять следующие обязанности:

- установить необходимые аппаратные средства, клиентское программное и информационное обеспечение, а также поддерживать их в работоспособном состоянии;
- выполнять требования по плановой смене ключей, своевременно уведомлять Удостоверяющий центр о компрометации криптографических ключей, а также соблюдать организационно-технические требования по обеспечению безопасности информации, установленные в Регламенте и Приложениях к нему;
- осуществлять оплату ЗАО «Роста» за услуги Удостоверяющего центра по изготовлению криптографических ключей и сертификатов ключей электронной подписи, в размере и в соответствии с порядком, установленным ЗАО «Роста»;
- соблюдать порядок разрешения конфликтных ситуаций и споров, установленный Регламентом;
- выполнять иные обязанности перед Удостоверяющим центром, возникающие в соответствии с Регламентом.

СТАТЬЯ 7. ВОЗНАГРАЖДЕНИЕ ЗА ПРЕДОСТАВЛЕНИЕ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ЗАО «РОСТА».

Вознаграждение за предоставление услуг Удостоверяющего Центра ЗАО «Роста»:

- вознаграждение устанавливается в размере 500 рублей, включая НДС, за каждый изготовленный сертификат ключа подписи и шифрования;
- в случае выполнения внеплановой смены ключей уполномоченного лица Удостоверяющего Центра (согласно процедуре, определенной в Регламенте) Удостоверяющий Центр выполняет изготовление сертификатов ключей подписи и шифрования Пользователей УЦ безвозмездно;
- размер вознаграждения Удостоверяющего Центра утверждается и вводится в действие ЗАО «Роста» только по предварительному уведомлению Пользователя Системы защищенного ЭДО;
- оплата осуществляется в российских рублях в безналичном порядке с использованием платежных поручений или иным способом, предусмотренным законодательством Российской Федерации. Размер рублевых денежных средств, подлежащих оплате, определяется по курсу доллара США, установленному ЦБ РФ на дату оплаты.

СТАТЬЯ 8. СРОКИ И ПОРЯДОК РАСЧЕТОВ.

Пользователь Системы ЭДО в течение 10 (десяти) банковских дней с даты выставления счета перечисляет ЗАО «Роста» или его партнеру, действующему от его имени на основании Договора поручения денежные средства в соответствии с размером вознаграждения, установленным настоящим договором.

СТАТЬЯ 9. ОТВЕТСТВЕННОСТЬ СТОРОН.

1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Договору Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

2. Стороны несут ответственность за действия своих сотрудников, а также иных лиц, получивших или имеющих доступ (независимо от того был ли этот доступ прямо санкционирован Стороной или произошел по ее вине) к используемым ими аппаратным средствам, программному, информационному обеспечению, криптографическим ключам, как за свои собственные.

СТАТЬЯ 10. СОГЛАСИТЕЛЬНЫЙ ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРОВ И РАЗНОГЛАСИЙ.

Все споры и разногласия, которые могут возникнуть в связи с применением, нарушением, толкованием настоящего Договора, признанием недействительным настоящего Договора или его части, стороны будут стремиться разрешить, используя механизмы согласительного урегулирования споров и разногласий.

СТАТЬЯ 11. СУДЕБНЫЙ ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ И РАЗНОГЛАСИЙ.

Если по итогам проведения согласительной процедуры конфликтная ситуация остается полностью или частично неурегулированной, стороны вправе разрешать неурегулированный спор и разногласия в соответствии с законодательством Российской Федерации.

СТАТЬЯ 12. СРОК ДЕЙСТВИЯ ДОГОВОРА.

1. Настоящий Договор заключен на неопределенный срок.
2. Настоящий Договор вступает в силу и становится обязательным для Сторон с момента его заключения.
3. Любая из договаривающихся Сторон вправе в одностороннем порядке расторгнуть настоящий Договор.
4. Настоящий Договор считается расторгнутым на следующий рабочий день после получения одной из Сторон письменного заявления о расторжении настоящего Договора, подписанного уполномоченным представителем другой Стороны.

СТАТЬЯ 13. ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ.

Все дополнения и изменения к настоящему Договору действительны в том случае, если они оформлены в письменном виде и подписаны уполномоченными представителями Сторон.

СТАТЬЯ 14. ПРОЧЕЕ.

1. Расторжение настоящего Договора не влияет на действительность и порядок действия документов, подписанных электронной подписью каждой из Сторон до даты расторжения Договора.
2. Термины, определение которых не приведено в тексте настоящего Договора, определяются в соответствии с Регламентом.

Реквизиты сторон:

Реквизиты ЗАО «Роста»:

Наименование:	Закрытое акционерное общество «Роста» ЗАО «Роста»
Юридический адрес:	344010, г. Ростов-на-Дону, пр. Ворошиловский, д. 52, оф 67
Почтовый адрес:	344010, г. Ростов-на-Дону, пр. Ворошиловский, д. 52, оф 67
Банковские реквизиты:	
-наименование банка	Ростовский филиал ОАО «Банк Москвы» г. Ростов-на-Дону
-расчетный счет	40702810500230001877
-корр. счет	30101810900000000991
-БИК	046015991

Реквизиты УЧАСТНИКА СЭД:

Наименование:	_____
Юридический адрес:	_____
Почтовый адрес:	_____
Банковские реквизиты:	_____
	_____
ИНН:	_____
:	

От ЗАО «Роста» Генеральный директор	От ……
_____ / В. Б. Кузнецов/	_____ /_____/
М.П.	М.П.

Приложение №2 к Регламенту

Генеральному директору ЗАО «Роста»
Кузнецову В.Б..
от _____
(должность руководителя , наименование организации)
_____
(ФИО руководителя)

ЗАЯВЛЕНИЕ
на регистрацию и изготовление сертификата ключа подписи
в Удостоверяющем центре

г. ___ Дата заявления «____» _____ 20___г.

Для работы в системе защищенного электронного документооборота (Системе ЗЭДО) прошу зарегистрировать и изготовить на имя уполномоченного лица сертификат ключа подписи в соответствии с указанными в настоящем заявлении данными:

Сведения о Пользователе СЗЭДО	Сведения об уполномоченном лице Пользователя СЗЭДО (ФИО Руководителя организации)
Полное наименование организации: _____ _____ Наименование организации: (заполняется **печатными латинскими** буквами) _____ Имя для использования в Системе ЗЭДО: (заполняется **печатными латинскими** буквами) _____ ОГРН: _____ ИНН / КПП:_____ Рег. № в ПФР: _____ Система налогообложения_____ (обычная, УСН, ЕНВД) а) Код ИФНС по местонахождению на учете: _____ б) Код ИФНС по месту осуществления деятельности:_____ E-mail: _____ (заполняется **печатными латинскими** буквами)	ФИО: _____ _____ Должность: _____ _____ ИНН: _____ Паспорт серия _____ номер _____ дата выдачи _____ выдан _____ _____ e-mail уполномоченного лица (для контактов): _____ тел/факс (для контактов): _____ Подпись уполномоченного лица _____
Адрес места расположения рабочего места Пользователя СЗЭДО – _____ _____ Правильность сведений, указанных в Заявлении, гарантирую. Руководитель _____ (фамилия, имя, отчество, должность руководителя) М.П. Подпись руководителя _____	

К заявлению Пользователя СЗЭДО прилагаются заверенные копии (копия верна, дата, подпись руководителя и печать организации) следующих документов:

1. Свидетельства о постановке на налоговый учет Налогоплательщика.
2. Свидетельства о постановке на налоговый учет уполномоченного лица (владельца сертификата).
3. Свидетельства о государственной регистрации Налогоплательщика, с присвоением ОГРН.
4. Приказа об организации работы в системе защищенного электронного документооборота.
5. Извещения о регистрации в территориальном органе ПФР.

Дата приема заявления сотрудником Удостоверяющего центра
«____» _____ 20____г.
_____ / _____/
(отметка ставится на экз. Удостоверяющего центра)

Приложение № 3 к Регламенту

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

«____» _____ 200__г.

_____ / _____
подпись

Приложение № 4 к Регламенту
Форма копии сертификата открытого
ключа подписи и шифрования на бумажном носителе

Наименование организации - Удостоверяющего Центра
Бланк сертификата ключа подписи и шифрования.

Данные Сертификата:
Версия: 3 (0x2)
Серийный Номер:40:00:00:00:4D:D7:59:44:48:3D:6B:11:0B:55:51:EA
Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
Издатель: CN=Rosta CA,O=Rosta,C=ru
Срок действия
Действителен с: 28 Май 2008 14:24:19 GMT
Действителен по: 26 Май 2013 23:59:00 GMT
Владелец: CN=Lychagin,O=Rosta,C=ru
Открытый Ключ Владельца:
Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
Открытый ключ ГОСТ 34.11-2001:
Параметры алгоритма:
Параметры открытого ключа: Параметры Диффи-Хеллман вариант провайдера
Параметры хэширования: Узел замены для хэша вариант провайдера
длина ключа: 512 бит
01:94:D1:56:4E:D8:95:73:01:97:E7:23:87:97:06:41:
23:FB:E1:EE:57:50:C8:B3:CF:08:E2:D2:D2:D6:86:71:
57:77:E6:F4:87:EC:6C:43:CD:CA:63:A8:B7:52:73:3D:
96:5D:47:50:53:EE:C6:0D:DB:1F:BF:39:FF:79:AD:6A
Дополнения X.509:
X509v3 Основные Ограничения:
CA:FALSE

Ссылка на Сертификат Регистрации:
Имя в директории:C=ru/O=Rosta/CN=Rosta RA
Серийный номер:40:00:00:00:D0:09:05:7D:45:F7:BA:6A:01:7D:D9:0D

X509v3 Идентификатор Ключа Владельца:
27:FC:ED:33:DC:1B:32:EC:7F:23:80:A2:B5:0E:18:3E:10:E3:B9:B2

Ссылка на предыдущий сертификат:
keyid:CF:21:EA:2C:B9:5F:78:CA:54:00:D5:B3:FE:00:8A:0D:DB:09:D8:BF
Имя в директории:C=ru/O=Rosta/CN=Rosta CA
Серийный номер:40:00:00:00:33:CA:A7:0D:45:F7:BD:02:01:87:F9:85

Идентификатор Закрытого ключа:
Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
Идентификатор Закрытого ключа: 1113L4SRJE01

X509v3 Область Применения Ключа:
Электронная Подпись
Шифрование Ключа
Шифрование Данных

X509v3 Альтернативное Имя Владельца:
Почтовый адрес RFC822:rosta-support@aaanet.ru
URI:www.rosta.rostov.ru
Организация:ЗАО "Роста"
Зарегистрированный Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф
.67
Фамилия:Лычагин Алексей Александрович
Должность:Администратор УЦ
Номер Телефона:(863)2994867, (863)2263104
Почтовый Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф.67

X509v3 Срок Действия Закрытого Ключа:
Действителен с:28 Май 2008 14:24:19 GMT
Действителен по:28 Авг 2009 23:59:00 GMT

X509v3 Расширенная Область Применения Ключа:
Защита эл. почты (1.3.6.1.5.5.7.3.4)

X509v3 Идентификатор Ключа Издателя:
keyid:67:EF:80:E7:A2:73:0B:B9:7F:6A:FD:B9:DE:BE:77:34:42:38:54:FB
Имя в директории:C=ru/O=Rosta/CN=Rosta CA
Серийный номер:40:00:00:00:3F:0E:1C:2B:48:3A:BE:80:0A:7C:24:71
X509v3 Точка Распространения COC:
URI:http://www.rosta.rostov.ru/certifying_center/vcert_mv/CN=RostaCA,O=Rosta,
C=ru.crl
X509v3 Альтернативное Имя Издателя:
URI:www.rosta.rostov.ru
Организация:ЗАО "Роста"
Зарегистрированный Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф
.67
Должность:Уполномоченное лицо ЦС
Номер Телефона:(863)2263104
Почтовый Адрес:344010, г.Ростов-на-Дону, пр.Ворошиловский, д.52, оф.67
Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
A6:DC:AC:9A:B9:FD:E4:D0:FA:EB:DD:4C:39:B5:6F:02:
A7:A0:44:EB:F0:E8:4F:99:F4:6E:D4:B0:BA:C3:4D:CD:
F0:5B:A5:70:62:09:0C:6B:35:83:A9:9A:6B:07:FC:28:
D3:6B:A8:33:87:DE:66:8C:14:12:0E:28:26:BA:F8:E9

Уполномоченное лицо _____ «___»_____200__г.

М. П.

Полномочный представитель организации _____ «__» _____200__г.
(владелец сертификата ключа электронной подписи)

Руководитель организации _____ «___» _____200__г.

М. П.

Приложение № 5 к Регламенту
Форма заявления на аннулирование
сертификата ключа
подписи и шифрования

ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ (ОТЗЫВ) СЕРТИФИКАТА КЛЮЧА ПОДПИСИ И ШИФРОВАНИЯ

_____
(наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

в связи с _____

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

просит аннулировать (отозвать) сертификат ключа подписи и шифрования серийный номер _____ _____, выданного на имя

_____
(фамилия, имя, отчество)

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

Владелец сертификата ключа подписи и шифрования _____
(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 подписи и шифрования _____ (Ф.И.О.) получено, личность _____ (Ф.И.О.) идентифицирована, сведения, указанные в Заявлении проверены.

«__» _____ 200__г.

Руководитель Удостоверяющего центра ЗАО «Роста» В. Б. Кузнецов.

Приложение №6 к Регламенту

Форма бланка запроса на сертификат

Система управления электронными сертификатами. VCERT MV.
Запрос на сертификат открытого ключа.

Запрос на Сертификат X.509:
Данные:
Версия: 1 (0x0)
Владелец: CN=Lychagin,O=Rosta,C=ru
Открытый Ключ Владельца:
Алгоритм Открытого Ключа: Подпись ГОСТ Р 34.10-2001
Открытый ключ ГОСТ 34.11-2001:
Параметры алгоритма:
Параметры открытого ключа: Параметры Диффи-Хеллман вариант провайдера
Параметры хэширования: Узел замены для хэша вариант провайдера
длина ключа: 512 бит
01:94:D1:56:4E:D8:95:73:01:97:E7:23:87:97:06:41:
23:FB:E1:EE:57:50:C8:B3:CF:08:E2:D2:D2:D6:86:71:
57:77:E6:F4:87:EC:6C:43:CD:CA:63:A8:B7:52:73:3D:
96:5D:47:50:53:EE:C6:0D:DB:1F:BF:39:FF:79:AD:6A
Атрибуты:
Время создания ЭЦП :28 Май 2008 14:22:54 GMT

Дополнения Запроса :
X509v3 Область Применения Ключа:
Электронная Подпись
Шифрование Ключа
Шифрование Данных

Ссылка на Сертификат Регистрации:
Имя в директории:C=ru/O=Rosta/CN=Rosta RA
Серийный номер:40:00:00:00:D0:09:05:7D:45:F7:BA:6A:01:7D:D9:0D

Идентификатор Закрытого ключа:
Идентификатор провайдера:СКЗИ Верба-OW версия 6.1
Идентификатор Закрытого ключа: 1113L4SRJE01

Ссылка на предыдущий сертификат:
keyid:CF:21:EA:2C:B9:5F:78:CA:54:00:D5:B3:FE:00:8A:0D:DB:09:D8:BF
Имя в директории:C=ru/O=Rosta/CN=Rosta CA
Серийный номер:40:00:00:00:33:CA:A7:0D:45:F7:BD:02:01:87:F9:85

Подпись открытого ключа:

4C:35:E6:1B:A8:BA:2C:D6:DF:10:B4:F1:AC:80:B5:1E:C5:06:92:BD:11:97:CC:BA:9B:

2A:18:9A:CE:AD:D5:6F:D9:4E:67:E3:B4:6C:F7:3F:D7:1E:58:D9:89:08:6D:11:AA:F4:
E2:40:20:B6:D0:D0:65:89:A4:63:2C:B4:22:04

X509v3 Идентификатор Ключа Владельца:
27:FC:ED:33:DC:1B:32:EC:7F:23:80:A2:B5:0E:18:3E:10:E3:B9:B2

Алгоритм ЭЦП: Подпись ГОСТ Р 34.10-2001 с хэш ГОСТ Р 34.11-94
59:EF:7F:4C:8D:09:B1:25:0B:06:AF:6D:2F:B1:77:F9:
88:92:0C:84:02:FB:28:E9:A9:C6:23:0C:1A:62:9C:CC:
D2:A8:CF:B4:57:60:DD:22:5A:EA:89:CE:9E:05:29:83:
F2:0E:F3:C4:F3:8F:65:91:50:BC:FC:1C:93:97:F3:DE

Представители организации:
Владелец открытого ключа _____ ___ _____ ____ г.
Руководитель организации _____ ___ _____ ____ г.
Главный бухгалтер _____ ___ _____ ____ г.

М.П.

Центр Регистрации:
Администратор _____ ___ _____ ____ г.

М.П.

Приложение №7 к Регламенту.

Журнал регистрации пользователей Удостоверяющего центра

п/п	Организация	Ф.И.О.уполномоченного лица пользователя системы	Лицензия регистрации (имя издателя и серийный номер)	Данные регистрации	Дата регистрации	Дата выбытия	Примечание
1	ЗАО «Роста»	Лычагин А.А..	CN=Lychagin,O=Rosta,C=ru 40:00:00:00:D0:09:05:7D:45:F7:BA:6A:01:7D:D9:0D	Имя для использования в системе…… ……. Почтовый адрес……. ……. Должность…… Ф.И.О…… Тел…….	14.03.2007		

Приложение№8 к Регламенту
. Журнал пользователя УЦ

п/п	Дата Время	Ф.И.О. пользователя системы	Событие	Дополнительные данные	Примечание