Приложение 7

РЕГЛАМЕНТ

получения сертификатов ключей подписи и использования электронной цифровой подписи

Дата: 9 августа 2010 года

УТВЕРЖДАЮ:

Генеральный директор ЗАО «Сбербанк-АСТ»

_____Ф.С. Кордыш

МП

Статс-секретарь,
заместитель Министра экономического развития Российской Федерации
_____А.В. Попова

Статс-секретарь,
Заместитель руководителя Федеральной антимонопольной службы
_____А.Ю. Цариковский

2010

Содержание

I. Основные термины

Для целей настоящего Регламента используются следующие основные понятия:

авторизация – процедура проверки Оператором удостоверяющего центра перед заключением с ним договора авторизации, заключение договора авторизации, внесение удостоверяющего центра в Единый реестр.

статус Авторизованного удостоверяющего центра(Авторизованный удостоверяющий центр) – полномочие удостоверяющего центра, дающее право на осуществление деятельности удостоверяющего центра в отношении участников размещения заказа.

Единый реестр – общий структурированный справочник, включающий:

– список Авторизованных удостоверяющих центров с указанием статуса (с Точками выдачи, перечнем корневых сертификатов);

– списки отозванных сертификатов ключей подписей участников размещения заказа, издаваемых Авторизованными удостоверяющими центрами, и указанием точек распространения списка отозванных сертификатов;

закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа

подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

точка выдачи сертификатов ключей подписи Авторизованного удостоверяющего центр (далее - Точка выдачи) - структурное подразделение Авторизованного удостоверяющего центра, либо организация, заключившая договор с Авторизованным удостоверяющим центром, осуществляющая выдачу сертификатов ключей подписи участникам размещения заказа, соответствующая законодательству РФ и требованиям настоящего Регламента, опубликованные в Единым реестре.

организация, ведущая Единый реестр – организация, уполномоченная в соответствии с распоряжением Правительства Российской Федерации №1231-р от 26.08.2009, на осуществление функций по ведению Единого реестра (ОАО Ростелеком);

пользователь Авторизованного удостоверяющего центра – физическое лицо, являющееся участником размещения заказа, либо физическое лицо, являющееся полномочным представителем юридического лица - участника размещения заказа, зарегистрированное в удостоверяющем центре и владеющее сертификатом ключа подписи, изданным удостоверяющим центром;

актуальный список отозванных сертификатов – список отозванных сертификатов на определённый момент времени, который действителен на такой момент времени;

точка распространения списка отозванных сертификатов – адрес в сети “Интернет”, на котором Авторизованный удостоверяющий центр осуществляет размещение актуального списка отозванных сертификатов.

сертификат ключа подписи уполномоченного лица удостоверяющего центра (далее корневой сертификат) – сертификат ключа подписи, выданный на физическое лицо, являющееся сотрудником удостоверяющего центра и наделенное удостоверяющим центром полномочиями по заверению сертификатов ключей подписей и списков отозванных сертификатов;

средство электронной цифровой подписи – аппаратное и (или) программное средство, обеспечивающее реализацию следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

Соглашение - соглашение о функционировании электронной площадки для проведения открытых аукционов в электронной форме в соответствии с главой 3.1 Закона, заключаемое между Министерством экономического развития Российской Федерации и Федеральной антимонопольной службой (с одной стороны) и оператором отобранной электронной площадки (с другой стороны);

Уполномоченный оператор электронной площадки (Уполномоченный оператор) – оператор электронной площадки, заключивший с удостоверяющим центром договор авторизации, обязанный обеспечить применение на электронных площадках сертификатов ключей подписей, изготовляемых удостоверяющим центром.

удостоверяющий центр – организация, осуществляющая выполнение целевых функций Удостоверяющего центра в соответствии с Федеральным законом «Об электронной цифровой подписи» от 10.01.2002 года № 1-ФЗ (деятельность удостоверяющего центра), а именно:

- изготавливает сертификаты ключей подписей;
- создает ключи электронных цифровых подписей с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдает сертификаты ключей подписей в форме документов на бумажных носителях и в форме электронных документов с информацией об их действии;
- осуществляет по обращениям участников размещения заказа, заказчиков, Контролирующих органов подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;

Кроме того в настоящем Регламенте используются термины и определения данные в Приложениях 1-4 к Соглашению.

II. Общие положения

2.1. Данный регламент является неотъемлемой частью Соглашения и определяет процесс изготовления и использования сертификатов ключей подписи участниками размещения заказа.

2.2. Регламент разработан в соответствии с Федеральным законом № 94-ФЗ от 21 июля 2005 г. «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

2.3. Регламент должен быть размещен в открытой части АС Оператора (на электронной площадке), а также на Официальном сайте.

2.4. Все иные документы Оператора электронной площадки не должны противоречить настоящему Регламенту.

2.5. Сертификаты ключей подписи, выданные в соответствии с настоящим Регламентом, используются для электронного документооборота при проведении электронных аукционов в соответствии с Законом 94-ФЗ.

III. Приобретение статуса Авторизованного удостоверяющего центра

3.1. Удостоверяющий центр, осуществляющий деятельность удостоверяющего центра в соответствии с настоящим Регламентом, должен быть авторизован в соответствии с настоящим Регламентом. Удостоверяющий центр, прошедший процедуру авторизации является Авторизованным удостоверяющим центром.

3.2. Авторизованный удостоверяющий центр обязан осуществлять деятельность удостоверяющего центра в соответствии с требованиями настоящего Регламента.

3.3. Сертификат ключа подписи участника размещения заказа, изготовленный Авторизованным удостоверяющим центром, действует на всех электронных площадках.

3.4. Удостоверяющий центр приобретает статус Авторизованного удостоверяющего центра после заключения предусмотренного разделом IX настоящего Регламента договора авторизации с Оператором электронной площадки, присоединению к Соглашению о взаимодействии операторов электронных площадок и Авторизованных удостоверяющих центров, предусмотренным в Приложении № 4 к настоящему Регламенту, и внесения сведений об удостоверяющем центре в Единый реестр.

3.5. Для начала процесса авторизации удостоверяющий центр должен подать оформленное в соответствии с Приложением № 2 к настоящему Регламенту заявление (далее - Заявление) одному из Операторов.

К Заявлению прикладываются нотариально заверенные копии следующих документов:

1) лицензии ФСБ России на деятельность по распространению (шифровальных) криптографических средств (срок окончания действия лицензии – не ранее трёх месяцев с момента подачи заявления на проведение авторизации);

2) лицензии ФСБ России на деятельность по техническому обслуживанию шифровальных (криптографических) средств (срок окончания действия лицензии – не ранее трёх месяцев с момента подачи заявления на проведение авторизации);

3) лицензий ФСБ России на деятельность по оказанию услуг в области шифрования информации (срок окончания действия лицензии – не ранее трёх месяцев с момента подачи заявления на проведение авторизации);

4) сертификата соответствия ФСБ России (система сертификации – РОСС RU.0001.030001) на используемое удостоверяющим центром средство автоматизации деятельности (сертификат соответствия должен устанавливать

класс обеспечения информационной безопасности указанного средства не ниже КС2);

а также,

5) копия уведомления о внесении в Единый государственный реестр сертификатов ключей подписей удостоверяющих центров сертификата уполномоченного лица удостоверяющего центра, заверенная руководителем удостоверяющего центра. Данное уведомление должно относиться к тому сертификату уполномоченного лица удостоверяющего центра, с использованием которого будут изготавливаться сертификаты ключей подписей для участников размещения заказа на электронных площадках;

3.6. На основании поступившего Заявления Оператором проводится проверка удостоверяющего центра на соответствие обязательным требованиям, предусмотренным в Приложении № 1 к настоящему Регламенту, а также требованиям, установленным Оператором электронной площадки, к соответствующему удостоверяющему центру.

Проверка удостоверяющего центра на соответствие требованиям, указанным в настоящем пункте, может осуществляться Оператором электронной площадки самостоятельно или организацией, с которой Оператор заключил соответствующий договор.

В течение срока рассмотрения Заявления Оператор обязан:

- проверить технологическую совместимость сертификатов ключей подписей, изготовленных удостоверяющим центром, подавшим Заявление, и программно-аппаратных комплексов действующих электронных площадок(технологическая совместимость);
- соответствие деятельности Удостоверяющего центра требованиям настоящего Регламента.

По результатам проверки составляется акт соответствия/не соответствия удостоверяющего центра требованиям настоящего Регламент и технологическую совместимость (далее Акт).

В случае направления запроса Контролирующим органом, Оператор в течение трёх рабочих дней обязан предоставить копию Акта.

Специальные условия проведения проверки и заключения договора авторизации указаны в пункте 3.26.

3.7. В случае, если оказание услуг по выдаче сертификатов ключей подписи для участников размещения заказа осуществляется обособленными подразделениями удостоверяющего центра, то в разделе «условия действия лицензии», лицензии выданной ФСБ России удостоверяющему центру, должны быть включены сведения об указанных обособленных подразделениях.

3.8. Удостоверяющий центр вправе заключить договор (соглашение) по делегированию части своих целевых функций, связанных с обеспечением выдачи сертификатов ключей подписей участников размещения заказа, с организацией, имеющей лицензии ФСБ России на виды деятельности, указанные в пункте 3.5 настоящего Регламента. В этом случае удостоверяющий центр должен приложить к Заявлению нотариально заверенные копии лицензий

ФСБ России на виды деятельности, указанные в пункте 3.5 настоящего Регламента, выданные соответствующей организации. Делегирование функций третьему лицу осуществляется по согласованию с Уполномоченным оператором.

Деятельность указанных в настоящем пункте организаций должна соответствовать положениям настоящего Регламента. При этом ответственность за действия указанных организаций несёт Авторизованный удостоверяющий центр.

3.9. В течение тридцати дней с момента поступления Заявления, Оператор должен направить два экземпляра, подписанного со своей стороны договора авторизации, либо отказать в авторизации.

3.10. Оператор электронной площадки вправе отказать в авторизации удостоверяющему центру без указания причин отказа, даже в случае наличия Акта.

3.11. После получения договоров авторизации от уполномоченного оператора Удостоверяющий центр должен в течение семи рабочих дней возвратить подписанные со своей стороны один экземпляр договора авторизации и заявление о присоединении к Соглашению о взаимодействии Операторов электронных площадок и Авторизованных удостоверяющих центров. С момента подписания договора Оператор становится Уполномоченным оператором для данного удостоверяющего центра. В качестве Уполномоченного оператора для каждого Удостоверяющего центра может выступать только один Оператор.

3.12. Уполномоченный оператор в течение одного дня со дня получения от удостоверяющего центра договора авторизации, направляет копию договора и копию заявления о присоединении к Соглашению о взаимодействии Операторов электронных площадок и Авторизованных удостоверяющих центров в виде электронного документа, заверенного электронно-цифровой подписью, в организацию, ведущую Единый реестр.

Также в организацию, ведущую Единый реестр, направляются корневой сертификат, список точек распространения списка отозванных сертификатов удостоверяющего центра, список Точек выдачи, адреса Точек выдачи, контактные телефоны Точек выдачи.

3.13. В течение одного дня со дня получения уведомления от Уполномоченного оператора, организация, ведущая Единый реестр, вносит информацию, указанную в пункте 3.12 настоящего Регламента, в Единый реестр и направляет уведомление об этом Уполномоченному оператору.

3.14. Удостоверяющий центр приобретает статус Авторизованного удостоверяющего центр с момента внесения сведений в Единый реестр.

3.15. Уполномоченный оператор в течение трех дней со дня приобретения удостоверяющим центром статуса Авторизованного удостоверяющего центра уведомляет других Операторов электронных площадок об Авторизованном удостоверяющем центре.

Уведомление Уполномоченного оператора должно содержать:

- наименование Авторизованного удостоверяющего центра;
- корневой сертификат Авторизованного удостоверяющего центра;
- точки распространения списка отозванных сертификатов(для каждого корневого сертификата);
- список Точек выдачи (с указанием адресов и контактных телефонов);

3.16. Авторизованный удостоверяющий центр имеет право начать выдавать сертификаты ключей подписей для участников размещения заказа не ранее чем через десять дней с момента приобретения статуса Авторизованного удостоверяющего центра. Если Авторизованный удостоверяющий центр в течении тридцати дней с момента получения статуса Авторизованного удостоверяющего центра не начал выдавать сертификаты ключей подписи в соответствии с требованиями настоящего Регламента, то договор авторизации считается расторгнутым.

3.17. С момента приобретения удостоверяющим центром статуса Авторизованного удостоверяющего центра, Уполномоченный оператор несёт субсидиарную ответственность за ущерб, причиненный таким Авторизованным удостоверяющим центром любым третьим лицам в связи с неисполнением, либо ненадлежащим исполнением своих обязательств по осуществлению деятельности удостоверяющего центра перед участниками размещения заказа на электронных площадках.(далее – субсидиарная ответственность Оператора)

Размер субсидиарной ответственности Оператора составляет семь миллионов рублей по каждому случаю нанесения ущерба третьим лицам.

3.18. Авторизованный удостоверяющий центр отвечает перед Оператором за убытки, причиненные Оператору вследствие неисполнения либо ненадлежащего исполнения Авторизованным удостоверяющим центром обязательств по осуществлению деятельности удостоверяющего центра перед участниками размещения заказа на электронных площадках.

3.19.Операторы не отвечают за ущерб, причиненный Авторизованным удостоверяющим центром любой третьей стороне неисполнением либо ненадлежащим исполнением обязательств по осуществлению деятельности удостоверяющего центра перед участниками размещения заказа на электронных площадках, осуществленной до получения удостоверяющим центром статуса Авторизованный удостоверяющий центр.

3.20. Размер ущерба, причиненного Авторизованным удостоверяющим центром третьей стороне неисполнением либо ненадлежащим исполнением обязательств, вытекающих из деятельности удостоверяющего центра перед участниками размещения заказа на электронных площадках определяется в судебном порядке в соответствии с законодательством Российской Федерации или может быть определен во внесудебном порядке по согласованию со всеми Операторами электронных торговых площадок.

3.21. Уполномоченный оператор или организация, с которой Оператор заключил соответствующий договор, обязаны осуществлять плановые проверки

не реже одного раза в календарный год, Авторизованного удостоверяющего центров на соответствие условиям настоящего Регламента, договора авторизации и требованиям законодательства Российской Федерации. По итогам каждой проверки составляется Акт в порядке, указанном в пункте 3.6 настоящего Регламента. Если договор авторизации заключен менее чем за три месяца до окончания календарного года, то плановая проверка в следующем году может не проводиться.

Кроме того, Уполномоченный оператор, или организация, с которой Оператор заключил соответствующий договор, вправе осуществлять внеплановые проверки Авторизованного удостоверяющего центра на соответствие условиям настоящего Регламента, договора авторизации и требованиям законодательства Российской Федерации. По итогам каждой проверки также составляется Акт в порядке, указанном в пункте 3.6 настоящего Регламента. Данная внеплановая проверка может осуществляться по требованию Минэкономразвития России, ФАС России.

3.22. Уполномоченный Оператор электронной площадки вправе потребовать от Авторизованного удостоверяющего центра предоставления финансового обеспечения ответственности Авторизованного удостоверяющего центра.

3.23. Статус Авторизованного удостоверяющего центра может быть приостановлен по основаниям, указанным в разделе IV настоящего Регламента, и прекращен по основаниям, указанным в разделе V настоящего Регламента.

3.24. В случае поступления в адрес Уполномоченного Оператора обоснованных претензий со стороны участников размещения заказа, Операторов, Контролирующего органа на действия Точки выдачи по выдаче сертификатов ключей подписей Авторизованного удостоверяющего центра, Уполномоченный оператор вправе исключить Точку выдачи из перечня Точек выдачи данного удостоверяющего центра по согласованию с Контролирующим органом, с одновременным уведомлением о исключении Точки выдачи организации, ведущей Единый реестр.

3.25. В случае появления новых Точек выдачи у Авторизованного удостоверяющего центра, Авторизованный удостоверяющий центр должен направить уведомление Уполномоченному оператору.

К уведомлению прикладываются нотариально заверенные копии документов указанных в пунктах 3.7 , 3.8 настоящего Регламента.

Уполномоченный оператор должен в течение тридцати дней с даты получения уведомления предоставить согласие, либо мотивированный отказ. В случае согласия Уполномоченный оператор осуществляет уведомление согласно пунктам 3.12, 3.15 настоящего Регламента. В случае получения отказа от Уполномоченного оператора Авторизованный удостоверяющий центр не вправе осуществлять деятельность удостоверяющего центра в отношении участников размещения заказа на электронных площадках в не согласованных Точках выдачи.

3.26. Если при проверке Удостоверяющего центра, подавшего Заявление, Оператор устанавливает, что данный Удостоверяющий центр имеет более шестидесяти Точек выдачи, Оператор направляет уведомления о получении такого Заявления всем другим Операторам. Получившие уведомление Операторы вправе направить согласие на функционирование данного удостоверяющего центра в качестве Общего Авторизованного удостоверяющего центра в течение пяти рабочих дней со дня направления уведомления. В этом случае все Операторы электронных площадок, выразившие согласие несут субсидиарную ответственность за ущерб, причиненный таким Общим Авторизованным удостоверяющим центром любым третьим лицам в связи с неисполнением, либо ненадлежащим исполнением обязательств по осуществлению деятельности удостоверяющего центра перед участников размещения заказа на электронных площадках.

Если Оператор не направил в установленном настоящим пунктом порядке согласие, то такой Оператор не несёт субсидиарную ответственность Оператора за Общий Авторизованный удостоверяющий центр.

Операторы, признавшие Общий Авторизованный удостоверяющий центр, в срок, установленный настоящим Регламентом, заключают многосторонний единый договор авторизации, при этом, если на стадии согласования между Операторами возникают разногласия по условиям договора авторизации, решение принимается большинством голосов Операторов. В этом случае формируется протокол принятия решения, который составляется в количестве семи экземпляров, два из которых направляются в Минэкономразвития России, ФАС России. Уполномоченным оператором для Общего Авториизованного удостоверяющего центра является Оператор, которому было подано Заявление.

Размер общей субсидиарной ответственности Операторов составляет семь миллионов рублей по каждому случаю нанесенного Общим Авторизованным удостоверяющим центром ущерба третьим лицам. Операторы, признавшие Общий Авторизованный удостоверяющий центр в соответствии с настоящим пунктом, несут субсидиарную ответственность Оператора в равных долях.

IV. Приостановление статуса Авторизованного удостоверяющего центра

4.1. Статус Авторизованного удостоверяющего центра приостанавливается Уполномоченным оператором по следующим основаниям:

а) подача Авторизованным удостоверяющим центром Уполномоченному оператору заявления о приостановлении статуса;

б) несоответствие Авторизованного удостоверяющего центра требованиям установленным в соответствии пунктом 3.6. настоящего Регламента;

в) получение Уполномоченным оператором обоснованных требований третьей стороны о взыскании с Оператора ущерба, причиненного неисполнением либо ненадлежащим исполнением Авторизованным

удостоверяющим центром обязательств по деятельности удостоверяющего центра перед участниками размещения заказа на электронных площадках;

г) задержка в публикации списка отозванных сертификатов более двух раз за месяц, либо не предоставление сведений о замене корневого сертификата в сроки, указанные в пункте 6.2 настоящего Регламента;

д) неисполнение или ненадлежащее исполнение Авторизованным удостоверяющим центром положений договора авторизации;

е) принятие учредителями (участниками) либо органом Уполномоченного оператора, уполномоченного на то учредительными документами, решения о ликвидации Уполномоченного оператора;

ж) вступившее в законную силу решение суда о признании банкротом Уполномоченного оператора,;

з) предписание ФАС России по результатам осуществления проверки Авторизованного удостоверяющего центра;

и) наложение на Уполномоченного оператора со стороны Контролирующего органа штрафов за нарушение требований Регламента со стороны Удостоверяющего центра три и более раз в течение одного календарного квартала.

4.2. Авторизованный удостоверяющий центр вправе приостановить статус Авторизованного удостоверяющего центра по своей инициативе путем направления письменного уведомления Уполномоченному оператору за тридцать дней до предполагаемой даты приостановления статуса.

В случае несоблюдения Авторизованным удостоверяющим центром тридцатидневного срока, его исчисление осуществляется со дня фактической отправки Удостоверяющим центром письменного уведомления Оператору.

4.3. Уполномоченный оператор не позднее одного дня с момента получения уведомления Авторизованного удостоверяющего центра о приостановлении статуса уведомляет об этом всех действующих Операторов электронных площадок, организацию, ведущую Единый реестр, и размещает сообщение о дате приостановления статуса на своем официальном сайте.

4.4. Статус Авторизованный удостоверяющий центр считается приостановленным со дня внесения сведений о приостановлении статуса в Единый реестр.

4.5. Организация, ведущая Единый реестр, не позднее одного дня с момента получения уведомления Уполномоченного оператора размещает на своем официальном сайте сообщение о дате приостановления у Удостоверяющего центра статуса Авторизованный удостоверяющий центр.

Организация, ведущая Единый реестр, вносит в Единый реестр сведения о приостановлении статуса Авторизованный удостоверяющий центр в соответствии с датой приостановления статуса, указанной в уведомлении Уполномоченного оператора.

4.6. В случае приостановления статуса Авторизованный удостоверяющий центр по основаниям, указанным в подпунктах б), в), г), д), е), ж), з), и) пункта

4.1. настоящего Регламента, Уполномоченный оператор в течение пяти рабочих дней с момента принятия решения уведомляет об этом соответствующий Удостоверяющий центр, всех действующих Операторов электронных площадок, организацию, ведущую Единый реестр, и размещает уведомление на своем официальном сайте.

4.7. В течение одного дня с момента получения уведомления Уполномоченного оператора о приостановлении статуса Авторизованного удостоверяющего центра Организация, ведущая Единый реестр, вносит в Единый реестр сведения о приостановлении статуса соответствующего Удостоверяющего центра и размещает сообщение о приостановлении статуса Удостоверяющего центра на своем официальном сайте.

4.8. Удостоверяющий центр со дня приостановления статуса Авторизованного удостоверяющего центра не вправе предоставлять услуги по изготовлению сертификатов ключей подписей для участников размещения заказа, при этом, такой центр обязан осуществлять функции по управлению сертификатами ключей подписей участников размещения заказа, изготовленных им до приостановления статуса.

4.9. Возобновление статуса Авторизованного удостоверяющего центра, приостановленного по основаниям, предусмотренным пунктом 4.1. настоящего Регламента, осуществляется не ранее чем через шесть месяцев с даты приостановления статуса Авторизованный удостоверяющий центр в порядке, предусмотренном разделом III настоящего Регламента.

4.10. Субсидиарная ответственность Оператора перед третьими лицами в соответствии с разделом III настоящего Регламента за неисполнение или ненадлежащее исполнение Удостоверяющим центром, статус Авторизованного удостоверяющего центра которого приостановлен, обязательств по деятельности удостоверяющего центра перед участниками размещения заказа на электронных площадках распространяется только на сертификаты, выданные указанным центром до даты приостановления статуса Авторизованного удостоверяющего центра.

Операторы электронных площадок обеспечивают размещение перечня Удостоверяющих центров с приостановленным статусом Авторизованного удостоверяющего центра на своих официальных сайтах.

С 1 января 2011 года размещение перечня Удостоверяющих центров с приостановленным статусом Авторизованного удостоверяющего центра осуществляется также на Официальном сайте.

4.11.При наличии оснований приостановления статуса Авторизованного удостоверяющего центра, указанных в подпунктах б), в), г), д), и) пункта 4.1. настоящего Регламента, Уполномоченный оператор имеет право не приостанавливать указанный статус, уведомив об этом в течение пятнадцати дней всех Операторов и Контролирующий орган. В течение шести месяцев с момента направления указанного уведомления Уполномоченный оператор несет субсидиарную ответственность Оператора в размере и порядке указанном в пункте 10.16 настоящего регламента.

V. Прекращение статуса Авторизованного удостоверяющего центра

5.1. Статус Авторизованного удостоверяющего центра прекращается по следующим основаниям:

а) прекращение срока действия (отзыва) всех сертификатов ключей подписей участников размещения заказа, изготовленных удостоверяющим центром до приостановления статуса Авторизованного удостоверяющего центра, если такой статус возобновлен не был;

б) прекращение деятельности Авторизованного удостоверяющего центра в порядке, установленном законодательством Российской Федерации;

в)наложение на Уполномоченного оператора со стороны Контролирующего органа штрафа за нарушение требований Регламента со стороны удостоверяющего центра, статус Авторизованного удостоверяющего центра которого приостановлен.

5.2. В случае наступления оснований для прекращения статуса Авторизованного удостоверяющего центра, согласно подпункту а) пункта 5.1. настоящего Регламента, Уполномоченный оператор в течение одного дня уведомляет об этом соответствующий удостоверяющий центр, других действующих Операторов электронных площадок, организацию, ведущую Единый реестр, и размещает уведомление на официальном сайте уполномоченного оператора.

5.3. В случае наступления оснований для прекращения статуса Авторизованного удостоверяющего центра, согласно подпунктам б), в) пункта 5.1. настоящего Регламента, сертификаты ключей подписей, выданные этим удостоверяющим центром, могут быть переданы в другой Авторизованный удостоверяющий центр по согласованию с Уполномоченным оператором и при отсутствии возражений от владельцев сертификатов ключей подписей не позднее одного месяца с момента прекращения статуса Авторизованный удостоверяющий центр. Если сертификаты ключей подписи были переданы были переданы в другой Авторизованный удостоверяющий центр, данный центр обязан уведомить в течение пяти рабочих дней о такой передаче Уполномоченного оператора, который направляет в течение пяти рабочих дней информацию об этом в организацию, ведущую Единый реестр.

Сертификаты ключей подписей, не переданные в другой авторизованный удостоверяющий центр, аннулируются.

5.4. Организация, ведущая Единый реестр, не позднее одного дня с момента получения уведомления от Уполномоченного оператора о прекращении у удостоверяющего центра статуса Авторизованного удостоверяющего центра, вносит в Единый реестр сведения о прекращении у соответствующего удостоверяющего центра указанного статуса.

5.5. Статус Авторизованного удостоверяющего центра прекращается с момента внесения сведений о прекращении статуса в Единый реестр.

5.6. Сертификаты ключей подписей, изготовленные удостоверяющим центром, статус Авторизованного удостоверяющего центра которого прекращен, не могут использоваться участниками размещения заказа на электронных площадках, за исключением тех сертификатов ключей подписей, которые были переданы в другой Авторизованный удостоверяющий центр согласно пункту 5.3 настоящего Регламента.

5.7. В случае прекращения у удостоверяющего центра статуса Авторизованного удостоверяющего центра договор авторизации считается расторгнутым.

5.8. Удостоверяющий центр, статус Авторизованного удостоверяющего центра которого прекращен, вправе вновь приобрести указанный статус не ранее чем через один год после прекращения, в порядке, предусмотренном разделом III настоящего Регламента.

5.9 Субсидиарная ответственность Оператора перед третьими лицами в соответствии с разделом III настоящего Регламента за неисполнение или ненадлежащее исполнение удостоверяющим центром, статус Авторизованного удостоверяющего центра которого прекращён, обязательств по деятельности удостоверяющего центра перед участниками размещения заказа на электронных площадках прекращается с даты прекращения указанного статуса.

5.11 В случае прекращения статуса Авторизованного удостоверяющего центра, согласно подпункту в) пункта 5.1. настоящего Регламента, владельцы сертификатов ключей подписей, изготовленные этим удостоверяющим центром, не переданные другому Авторизованному удостоверяющему центру согласно пункту 5.3 настоящего Регламента вправе обратиться с требованием компенсации суммы средств, затраченных на получение сертификата ключей подписи, к удостоверяющему центру, статус Авторизованного удостоверяющего центра которого прекращен.

VI. Взаимодействие авторизованных удостоверяющих центров и операторов электронных площадок.

6.1. Авторизованный удостоверяющий центр обязан ежедневно публиковать в точках распространения списков отозванных сертификатов и направлять Уполномоченному оператору актуальный список отозванных сертификатов ключей подписей участников размещения заказа. Авторизованный удостоверяющий центр согласовывает время направления списка отозванных сертификатов ключей подписей с Уполномоченным оператором. При этом, в случае отзыва сертификата ключа подписи участника размещения заказа, Авторизованный удостоверяющий центр обязан опубликовать в точках распространения списков отозванных сертификатов и направить Уполномоченному оператору обновлённый список отозванных сертификатов в течении тридцати минут после поступления в Авторизованный удостоверяющий центр от участника размещения заказа заявления на отзыв сертификата ключа подписи. В случае невыполнения Авторизованным

удостоверяющим центром положений настоящего пункта, Операторы используют последний список отозванных сертификатов ключей подписей, предоставленный Авторизованным удостоверяющим центром, за исключением случая указанного, в пункте 8.17 настоящего Регламента.

6.2. В случае смены ключей подписей и изготовления нового корневого сертификата Авторизованный удостоверяющий центр обязан в течение одного часа направить уполномоченному оператору новый корневой сертификат.

6.3 Уполномоченный оператор при получении сведений от Авторизованного удостоверяющего центра, предусмотренных в пункте 6.1 настоящего Регламента, в течении одного часа с момента получения сведений передает их организации, ведущей Единый реестр.

6.4. Уполномоченный оператор при получении сведений от Авторизованного удостоверяющего центра, предусмотренных в пункте 6.2 и настоящего Регламента, в течении одного рабочего дня с момента получения сведений передает их организации, ведущей Единый реестр.

6.5 Операторы должны обеспечить актуализацию списка отозванных сертификатов ключей подписей и корневых сертификатов Авторизованных удостоверяющий центров в АС Оператора посредством организации регулярных обращений в Единый реестр.

6.6. Функции по передаче сведений от Авторизованных удостоверяющих центров Уполномоченному оператору (пункт 6.1, пункт 6.2 настоящего Регламента, а также иных сведений, предусмотренных настоящим Регламентом), могут быть переданы организации, располагающей необходимыми техническими и аппаратно-программными средствами, по согласованию Авторизованного удостоверяющего центра и Уполномоченного оператора. Ответственность за полноту и достоверность передаваемой информации в этом случае несёт Уполномоченный удостоверяющий центр.

6.7. Функции по передаче сведений от Уполномоченного оператора организации, ведущей Единый реестр (пункты 6.3, 6.4 настоящего Регламента), могут быть переданы организации, располагающей необходимыми техническими и аппаратно-программными средствами, по согласованию уполномоченного оператора и организации, ведущей Единый реестр, при этом ответственность за своевременность, полноту и достоверность передаваемой информации несёт Уполномоченный оператор.

6.8. Авторизованный удостоверяющий центр вправе проводить регламентные работы. Не менее чем за семь дней до начала проведения регламентных работ Авторизованный удостоверяющий центр должен уведомить Уполномоченного оператора о проведении таких работ с указанием точной даты и времени их начала и окончания. При этом дата и время проведения регламентных работ могут приходиться только на выходные и праздничные дни с таким расчетом, чтобы начало регламентных работ приходилось не ранее чем на 01:00 московского времени первого выходного (праздничного) дня, следующего за рабочим днем, а окончание регламентных работ приходилось не позднее чем на 15:00 московского времени последнего

перед рабочим выходного дня. Конкретную дату и время проведения регламентных работ Авторизованный удостоверяющий центр определяет самостоятельно, без согласования с Уполномоченным оператором.

6.9. Уполномоченный оператор электронной площадки обязан размещать информацию, предусмотренную настоящим пунктом, на официальном сайте Уполномоченного оператора в сети "Интернет" :

– списка Авторизованных удостоверяющих центров данного Уполномоченного оператора с указанием статуса, а также точек выдачи и перечнем корневых сертификатов(с указанием контактных телефонов и адресов);

– списка отозванных сертификатов ключей подписей участников размещения заказа, издаваемых Авторизованными удостоверяющими центрами данного Уполномоченного оператора, и адреса их публикации в сети “Интернет”.

Размещение информации, предусмотренной настоящим пунктом должно осуществляться не позднее тридцати минут с момента получения сведений от Авторизованного удостоверяющего центра.

6.10. Оператор обязан обеспечить работу с действительными сертификатами ключей подписей, изготовленными:

– Авторизованными удостоверяющими центрами, выполняющими требования установленные настоящим Регламентом;

– удостоверяющими центрами с приостановленным статусом Авторизованный удостоверяющий центр, изготовленными до момента приостановления статуса Авторизованный удостоверяющий центр;

– до 1 января 2011 года удостоверяющими центрами, указанными в пункте 11.1. настоящего Регламента;

– удостоверяющим центром Федерального казначейства.

6.11. Оператор электронной площадки обязан осуществлять проверку подлинности сертификатов открытых ключей электронных цифровых подписей участников размещения заказа. Необходимыми условиями для признания сертификат ключа подписи подлинным, являются следующие:

-на момент формирования электронной цифровой подписи сертификат ключа подписи не внесен в список отозванных сертификатов, опубликованных в Едином реестре,

-корневой сертификат Авторизованного удостоверяющего центра, выдавшего данный сертификат ключа подписи, внесён в Единый реестр,

-сертификат ключа подписи выдан до даты приостановления статуса Авторизованного удостоверяющего центра.

6.12. Оператор при отсутствии обновления Авторизованным удостоверяющим центром списка отозванных сертификатов ключей подписи обязан в течении десяти минут после истечения срока обновления, уведомить всех участников размещения заказа, находящихся на стадии подписании государственного контракта на электронной площадке Оператора, и использующих сертификаты ключа подписи данного Авторизованного

удостоверяющего центра. Уведомление осуществляется через личный кабинет участника размещения заказа.

6.13 Уполномоченный оператор обязан обеспечить выполнение Авторизованным удостоверяющим центром требований, предусмотренных пунктами 6.1, 6.2, 6.8 настоящего Регламента.

VII. Ведение Единого реестра

7.1. Организация, ведущая Единый реестр, обязана в течение одного часа с момента получения от Уполномоченного оператора указанных в настоящем Регламенте данных внести их в Единый реестр.

7.2. Организация, ведущая Единый реестр, обеспечивает круглосуточное размещение информации содержащейся в Едином реестре на своем официальном сайте в сети "Интернет", а с 1 января 2011 года также на Официальном сайте.

VIII. Порядок использования электронной цифровой подписи при осуществлении электронного документооборота при проведении открытых аукционов в электронной форме и взаимодействии авторизованных удостоверяющих центров и операторов электронных площадок

8.1. Использование электронной цифровой подписи осуществляется в соответствии с Федеральным законом № 1-ФЗ от 10 января 2002 г. «Об электронной цифровой подписи» и настоящим Регламентом.

8.2. Обмен электронными документами, подписанными электронной цифровой подписью является юридически значимым электронным документооборотом.

8.3. Исчисление сроков, предусмотренных настоящим Регламентом, если иное не оговорено специально, начинается с момента отправки электронного документа.

8.4. Операторы электронных площадок, Авторизованные удостоверяющие центры, Удостоверяющий центр Федерального Казначейства, Организация, ведущая единый реестр, уполномоченный федеральный орган исполнительной власти в сфере размещения заказа и другие субъекты правовых взаимоотношений, регулируемых настоящим Регламентом, несут ответственность за сохранность и использование надлежащим образом закрытых ключей электронных цифровых подписей для информационного обмена в соответствии с действующим законодательством Российской Федерации.

8.5. Все документы и сведения, связанные с приобретением, приостановлением и прекращением у Удостоверяющего центра статуса Авторизованный удостоверяющий центр, взаимодействием между Операторами электронных площадок, Авторизованными удостоверяющими центрами, Удостоверяющим центром Федерального Казначейства, Организацией, ведущей единый реестр, уполномоченным федеральным органом исполнительной власти в сфере размещения заказа и другими субъектами правовых взаимоотношений, регулируемых настоящим Регламентом, если иное не оговорено специально, должны быть в форме электронных документов.

8.6. Электронный документ, подписанный электронной цифровой подписью, имеет такую же юридическую силу, как и подписанный собственноручно документ на бумажном носителе, и влечет предусмотренные для указанного документа правовые последствия.

Наличие в электронном документе электронной цифровой подписи организаций и органов, указанных в пункте 8.4 настоящего Регламента, означает, что документ направлен от их имени, а сведения, содержащиеся в нем, являются подлинными и достоверными.

8.7. Документы, размещаемые на официальном сайте, должны быть подписаны электронной цифровой подписью лица, имеющего право действовать от имени соответствующей организации (органа).

8.8. Электронные документы, заверенные электронной цифровой подписью, направляются на электронные почтовые ящики, указанные на официальных сайтах соответствующих организаций (органов) и в случае, если возможно технически обеспечить, то данный электронный документ дублируется в личный кабинет соответствующей организации (органов).

В иных случаях Операторы, Авторизованный удостоверяющий центр, Удостоверяющий центр Федерального Казначейства, Организация, ведущая единый реестр, уполномоченный федеральный орган исполнительной власти в сфере размещения заказа и другие субъекты правовых взаимоотношений, регулируемых настоящим Регламентом, обязаны уведомить контрагента о своих электронных почтовых ящиках, предназначенных для информационного обмена.

8.9. Сертификаты ключей подписей, используемые при осуществлении электронного документооборота при проведении открытых аукционов в электронной форме должны изготавливаться только Авторизованными удостоверяющими центрами, за исключением случая указанного в пункте 11.1 настоящего Регламента.

8.10. Сертификат ключа подписи признается действительным, если соответствует настоящему Регламенту, а также следующим требованиям:

- для данного сертификата ключа подписи подтверждена подлинность электронной цифровой подписи с использованием корневого сертификата и средства электронной цифровой подписи;

- корневой сертификат содержится в Едином реестре;

- данный сертификат ключа подписи отсутствует в актуальном списке отозванных сертификатов ключей подписей Авторизованного удостоверяющего центра;

8.11. Средства применения электронной цифровой подписи должны соответствовать настоящему регламенту, а также:

- обеспечить реализацию функций создания электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждения с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создания закрытых и открытых ключей электронных цифровых подписей, используется средство криптографической защиты информации, сертифицированное в системе сертификации РОСС RU.0001.030001.

- использоваться совместно со средствами вычислительной техники, общесистемным программным обеспечением и его компонентами, а также иным программно-аппаратным и информационным обеспечением, необходимым для осуществления электронного документооборота при проведении открытых аукционов в электронной форме и для обеспечения информационного обмена между Авторизованными удостоверяющими центрами, Операторами электронных площадок, участниками размещения заказа и Контролирующими органами.

- применяться в соответствии с требованиями эксплуатационной документации на данное средство электронной цифровой подписи (средство криптографической защиты информации).

- обеспечивать формирование электронной цифровой подписи в формате, определяемом рекомендациями RFC 3852 «Cryptographic Message Syntax (CMS)», с учетом использования криптографических алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 в соответствии с RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

8.12. Участники размещения заказа самостоятельно обеспечивают сохранность в тайне закрытых ключей электронных цифровых подписей, и несут за это ответственность в соответствии с действующим законодательством Российской Федерации.

8.13. Порядок формирования и проверки электронной цифровой подписи должен соответствовать следующим основным требованиям:

1)Формирование электронной цифровой подписи электронного документа осуществляется с использованием средств применения электронной цифровой подписи.

2)Формирование электронной цифровой подписи должно осуществляться только с использованием действующего закрытого ключа подписи.

3)Подтверждение подлинности электронной цифровой подписи электронного документа осуществляется с использованием средств применения электронной цифровой подписи.

4)При подтверждении подлинности электронной цифровой подписи должна осуществляться проверка, что электронная цифровая подпись в электронном документе равнозначна собственноручной (должно осуществляться выполнение условий равнозначности электронной цифровой подписи собственноручной), и только после признания электронной цифровой подписи равнозначной собственноручной может быть осуществлено исполнение данного электронного документа.

8.14.Формирование электронного документа осуществляется с учётом следующих требований:

1) Создание электронных документов осуществляется надлежаще уполномоченными лицами;

2) Сертификат ключа подписи уполномоченного на совершение указанного действия лица должен содержать сведения, устанавливающие право владельца данного сертификата формировать электронную цифровую подпись данного типа электронных документов;

3) Порядок применения участниками размещения заказа и государственными (муниципальными) заказчиками электронной цифровой подписи в электронных документах, используемых при проведении открытого аукциона в электронной форме, определяется Регламентом организации и проведения открытых аукционов в электронной форме для размещения заказов на поставку товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд;

4) При взаимодействии Авторизованных удостоверяющих центров, участников размещения заказа, Контролирующих органов и Операторов допускается использование сканированных бумажных документов, подписанных электронной цифровой подписью с использованием средств применения электронной цифровой подписи и сертификата ключа подписи уполномоченного на совершение данного действия лица. При этом под сканированным бумажным документом понимается электронный образ бумажного документа, созданный с помощью специальных средств, обеспечивающих преобразование изображения на бумажном носителе в цифровую форму. Результатом сканирования бумажного документа является файл, содержащий графическое изображение данного бумажного документа. Допускается применение следующих форматов графических файлов - Joint Photographic Experts Group (расширение файла - JPG), Portable Document Format (расширение файла - PDF), Bitmap Picture(расширение файла - BMP), Graphics Interchange Format (расширение файла - GIF), Tagged Image File Format (расширение файла - TIFF), Photoshop Document (расширение файла - PSD),

portable network graphics (расширение файла -PNG), Encapsulated PostScript (расширение файла - EPS), DjVu (расшириение файла - DjVu).

8.15. В настоящем Регламенте применяются следующие требования к применению электронной цифровой подписи.

1) сертификат ключа подписи действует на определенный момент времени (действительный сертификат), если:

– сертификат ключа подписи издан авторизованным удостоверяющим центром либо удостоверяющим центром, указанным в п. 11.1 настоящего Регламента;

– подтверждена подлинность электронной цифровой подписи уполномоченного лица авторизованного удостоверяющего центра либо уполномоченного лица удостоверяющего центра, указанного в п. 11.1 настоящего Регламента;

– наступил момент времени начала действия сертификата ключа подписи;

– срок действия сертификата ключа подписи не истек;

– сертификат ключа подписи отсутствует в актуальном списке отозванных сертификатов, опубликованном в Едином реестре сертификатов ключей подписей, либо на официальном сайте в сети “Интернет” уполномоченного оператора;

2) закрытый ключ подписи действует на определённый момент времени (действительный закрытый ключ), если:

– наступил момент времени начала действия закрытого ключа;

– срок действия закрытого ключа не истек;

– сертификат ключа подписи, соответствующий данному закрытому ключу, действует на данный момент времени (является действительным).

3) Электронная цифровая подпись в электронном документе действительна при одновременном соблюдении следующих условий:

а) на момент формирования электронной цифровой подписи электронного документа:

– сертификат ключа подписи, относящийся к электронной цифровой подписи, являлся действительным;

– закрытый ключ, соответствующий указанному сертификату ключа подписи, являлся действительным;

б) подтверждена подлинность электронной цифровой подписи электронного документа на сертификате, относящемся к данной электронной цифровой подписи;

в) электронная цифровая подпись электронного документа сформирована в соответствии со сведениями, указанными в сертификате ключа подписи: сертификат ключа подписи в расширениях Extended Key Usage, Certificate Policies содержит области использования сертификата и ключа, устанавливающие право владельца данного сертификата ключа подписи подписывать соответствующие электронные документы. Перечень областей использования сертификатов ключей подписей устанавливается

уполномоченным федеральным органом исполнительной власти в сфере размещения заказа.

8.16. Если на момент времени начала проведения открытого аукциона или в течение времени проведения открытого аукциона оператор электронной площадки не может установить статус сертификата ключа подписи участника открытого аукциона по причине отсутствия актуального списка отозванных сертификатов, то оператор площадки признает сертификат ключа подписи участника размещения заказа действительным.

8.17. Если при подписании электронной цифровой подписи участником размещения заказа государственного контракта оператор электронной площадки не может установить статус сертификата ключа подписи участника размещения заказа по причине отсутствия актуального списка отозванных сертификатов (не предоставление актуального списка отозванных сертификатов Авторизованным удостоверяющим центром), то оператор площадки признает сертификат ключа подписи – не действительным. При этом участник размещения заказа, с которым заключается контракт, вправе подписать данный контракт электронной цифровой подписью с использованием сертификата ключа подписи, изданного другим Авторизованным удостоверяющим центром, либо обжаловать действия оператора электронной площадки в соответствии с 94-ФЗ.

IX. Договор авторизации

9.1 Договор авторизации между Уполномоченным оператором и удостоверяющим центром (далее договор авторизации) является договором присоединения в соответствии с пунктом 428 ГК РФ.

Вместе с тем, договор авторизации не является договором присоединения, если в соответствии с настоящим Регламентом он заключается в виде трёхстороннего или многостороннего документа, сторонами которого являются Уполномоченный оператор, удостоверяющий центр, а также организации, привлечённые для выполнения отдельных функций Оператора и удостоверяющего центра в случаях, предусмотренных настоящим Регламентом.

9.2. В договор авторизации должны быть включены все требования настоящего Регламента, касающиеся деятельности Авторизованного удостоверяющего центра.

9.3. Договор авторизации должен предусматривать в качестве требования к удостоверяющему центру обязательство присоединения к Соглашению о взаимодействии операторов электронных площадок и Авторизованных удостоверяющих центров указанное в Приложении № 4 к настоящему Регламенту.

9.4. Договор авторизации должен предусматривать ответственность Авторизованного удостоверяющего центр за:

– неисполнение или ненадлежащее исполнение обязательств и положений, установленных договором авторизации;

– приём, обработку и хранение документов, предоставляемых юридическими и физическими лицами для получения сертификата ключа подписи в Авторизованном удостоверяющем центре в целях участия в открытых аукционах в электронной форме на электронных площадках. При этом обработка документов должна предусматривать все необходимые и достаточные меры для установления подлинности предоставленных документов;

– соответствие сведений, вносимых в сертификаты ключей подписей, предоставленным для получения сертификата ключа подписи документам;

– своевременное уведомление Уполномоченного оператора в соответствии с пунктом 6.1 и пунктом 6.2 настоящего Регламента;

9.5. Договор авторизации должен предусматривать внесение обеспечительных взносов в Обеспечительный фонд и возврат средств из Обеспечительного фонда в порядке, предусмотренным разделом X настоящего Регламента.

9.6. Договор авторизации, направляемый Уполномоченным оператором авторизуемому удостоверяющему центру, может также включать:

- требование об обеспечении ответственности удостоверяющего центра перед Уполномоченным оператором
- ответственность удостоверяющего центра за ущерб, причиненный уполномоченному оператору неисполнением либо ненадлежащим исполнением обязательств деятельности удостоверяющего центра для участников размещения заказа на электронных площадках.

9.7. При прекращении договора авторизации, Оператор электронной площадки возвращает Удостоверяющему центру, обеспечение ответственности предоставленное удостоверяющим центром при заключении договора авторизации.

Обеспечение возвращается в полном размере за вычетом взысканных в соответствии с договором авторизации неустоек сумм, уплаченных Оператором по требованиям третьих лиц, но не возмещённых со стороны удостоверяющего центра. Возвращение обеспечения происходит только после прекращения всех требований третьих лиц, но не ранее чем через три месяца с момента прекращение договора авторизации.

X Обеспечительный Фонд.

10.1. Обеспечительный фонд создаётся за счёт обеспечительных взносов, перечисляемых Авторизованными удостоверяющими центрами Уполномоченному оператору на условиях возвратности. Обеспечительный взносы перечисляется по итогам календарного месяца исходя из количества выданных в этом месяце Авторизованным удостоверяющим центром сертификатов ключей подписи.

10.2. Размер обеспечительного взноса составляет двести пятьдесят рублей за каждый сертификат ключа подписи для участника размещения заказа, выданного Авторизованным удостоверяющим центром, кроме случая, указанного в пункте 10.6 настоящего Регламента. Внесение сумм обеспечительных взносов осуществляется Авторизованным удостоверяющим центром до пятого числа месяца следующего за отчётным.

10.3.Уполномоченный оператор перечисляет сумму полученных взносов на счёт Обеспечительного фонда до десятого числа месяца следующего за отчётным.

10.4. Ведение Обеспечительного фонда осуществляется Операторами в соответствии с указанной ниже очерёдностью:

С 01.01.11 по 01.01.12 ЗАО «Сбербанк – Автоматизированная Система Торгов»

С 01.01.12 по 01.01.13 ОАО «Единая электронная торговая площадка»

С 01.01.13 по 01.01.14 ГУП «Агентство по государственному заказу, инвестиционной деятельности и межрегиональным связям Республики Татарстан»

С 01.01.14 по 01.01.15 ООО «Индексное агентство РТС»

С 01.01.15 до даты окончания действия Соглашения ЗАО «ММВБ-Информационные технологии»

10.5. Средства Обеспечительного фонда могут быть использованы только для выплаты по требованиям третьих лиц, вытекающим из неисполнения или ненадлежащего исполнения обязательств по деятельности Авторизованного удостоверяющего центра перед участниками размещения заказа.

10.6. В случае если после выплат по требованию третьих лиц размер Обеспечительного фонда становится меньше минимального уровня, то размер обеспечительного взноса перечисляемого за каждый сертификат ключа подписи увеличивается до пятисот рублей до момента достижения Обеспечительном фондом минимального уровня.

10.7. Минимальный уровень Обеспечительного фонда составляет 50 миллионов рублей.(далее Минимальный уровень)

10.8. Требования третьих лиц, оставшиеся неудовлетворёнными после выплаты предельной суммы субсидиарной ответственности Оператора, могут быть удовлетворены за счёт средств Обеспечительного фонда.

В случае если размер Обеспечительного фонда составляет сумму равную минимальному уровню Обеспечительного фонда или менее, предельная сумма подлежащая выплате из Обеспечительного фонда за неисполнение либо ненадлежащее исполнение Авторизованным удостоверяющим центром обязательств по деятельности удостоверяющего центра для участников размещения заказа по каждому случаю нанесенного ущерба третьим лицам составляет семь миллионов рублей, в случае превышения размера Обеспечительного фонда свыше Минимального уровня, предельная сумма подлежащая выплате из Обеспечительного фонда за неисполнение либо ненадлежащее исполнение Авторизованным удостоверяющим центром

обязательств по деятельности удостоверяющего центра для участников размещения заказа по каждому случаю нанесенного ущерба третьим лицам составляет пятнадцать миллионов рублей.

10.9. Организация, ведущая учёт Обеспечительного фонда, обязана ежемесячно направлять информацию о размере Обеспечительного фонда в ФАС России и Минэкономразвития России.

10.10. Организация, ведущая учёт Обеспечительного фонда, обязана предоставлять информацию о размере Обеспечительного фонда по официальному запросу Операторов, Авторизованных удостоверяющих центров, Сторон соглашения.

10.11. В случае прекращения Договора авторизации Удостоверяющий центр вправе получить сумму обеспечительных взносов, перечисленную в Обеспечительный фонд.

10.12. Для получении обеспечения удостоверяющий центр направляет Уполномоченному оператору соответствующее заявление.

10.13. Уполномоченный оператор и Оператор, осуществляющий ведение Обеспечительного фонда в течение трёх месяцев рассматривают заявление удостоверяющего центра и при наличии оснований принимают решение о выплате, либо предоставляют мотивированный отказ. В случае положительного решения в течении трёх дней Оператор, ответственный за ведение Обеспечительного фонда, выплачивает Уполномоченному оператору сумму обеспечительных взносов. Уполномоченный оператор выплачивает сумму обеспечительных взносов в течении трёх дней после получения средств от Оператора, осуществляющего ведение Обеспечительного фонда.

10.14. Обеспечительные взносы возвращаются в полном размере за вычетом, суммы средств уплаченных Оператором, осуществляющим ведение Обеспечительного фонда, по требованиям третьих лиц. Возвращение суммы обеспечительных взносов происходит только после прекращения всех требований третьих лиц, но не ранее чем через три месяца с момента направления заявления указанного в пункте 10.12 настоящего Регламента.

10.15. Денежные средства в виде банковского процента полученные от кредитной организации, в которой открыт счёт для учёта средств Обеспечительного фонда, распределяются следующим образом. Двадцать процентов начисленных средств подлежат передаче Оператору осуществляющему ведение Обеспечительного Фонда. Восемьдесят процентов направляются на увеличение средств Обеспечительного фонда.

10.16. В случае указанном в пункте 4.11 настоящего Регламента Уполномоченный оператор несёт субсидиарную ответственность Оператора в размере 14 миллионов рублей, если размер Обеспечительного фонда не достиг Минимального уровня, либо в размере 22 миллионов рублей, если размер Обеспечительного Фонда превысил Минимальный уровень. Обеспечительный Фонд в этом случае освобождается от субсидиарной ответственности по отношению к данному Авторизованному удостоверяющему центру.

XI. Заключительные и переходные положения

11.1. Сертификат ключа подписи и соответствующий ему закрытый ключ, изготовленные для участника размещения заказа неавторизованным удостоверяющим центром до вступления в силу настоящего Регламента и действительные на электронной площадке (электронных площадках) до 01.07.2010, могут использоваться на данной электронной площадке (электронных площадках) в пределах срока своего действия, но не позднее 01.01.2011 года.

11.2. Владелец сертификата ключа подписи, указанного в пункте 11.1 настоящего Регламента, вправе до 01.01.2011 года изготовить на возмездной основе сертификат ключа подписи в авторизованном удостоверяющем центре в порядке, установленном настоящим Регламентом. В этом случае сертификат ключа подписи, полученный в неавторизованном удостоверяющем центре, считается недействительным на электронных площадках и не может применяться.

11.3. Оператор электронной площадки должен обеспечить направление уведомлений участникам размещения заказа о периоде действия сертификатов ключей подписей, за три месяца, тридцать дней, семь дней и один день до окончания срока действия сертификата ключа на электронную почту указанную при авторизации и в личный кабинет участника размещения заказа на электронной площадке.

11.4. Если на момент вступления настоящего Регламента в силу, организация, ведущая Единый реестр, не назначена в установленном законом порядке, то функции указанной организации в отношении авторизованного удостоверяющего центра, предусмотренные настоящим Регламентом, осуществляет уполномоченный оператор.

11.5. До назначения организации, ведущей Единый реестр, применяются следующие особенности:

1)Удостоверяющий центр приобретает статус Авторизованный удостоверяющий центр с момента подписания с уполномоченным оператором договора авторизации.

2)Статус Авторизованный удостоверяющий центр удостоверяющего центра считается приостановленным со дня размещения уведомления о приостановлении статуса на официальном Интернет-сайте уполномоченного оператора.

3)Удостоверяющий центр лишается статуса Авторизованного удостоверяющий центр со дня размещения уведомления о прекращении статуса на официальном Интернет-сайте уполномоченного оператора.

4)Сертификат ключа подписи признается подлинным, если он на момент формирования электронной цифровой подписи не внесен в список отозванных сертификатов ключей подписи, опубликованный официальном сайте в сети "Интернет" уполномоченного оператора.

5)Уполномоченный оператор при получении сведений от Авторизованного удостоверяющего центра, предусмотренных в пунктах 6.1, 6.2. настоящего Регламента, в течении одного часа размещает их на своем официальном сайте в сети «Интернет», а также направляет их другим операторам электронных площадок.

11.6. Каждый оператор электронной площадки обязан до 01.01.2011 года обеспечить наличие не менее одной Точки выдачи Авторизованных удостоверяющих центров в не менее чем пятнадцати субъектах Российской Федерации. Для выполнения требований данного пункта не учитываются Общие удостоверяющие центры являющиеся таковым для всех Операторов. В случае, если удостоверяющий центр является Общим удостоверяющим центром не для всех Операторов, то его Точки выдачи учитываются только у Операторов, которые приняли данный удостоверяющий центр в качестве Общего удостоверяющего центра, в количестве Точек выдачи делённое на количество Операторов, которые приняли данный удостоверяющий центр в качестве Общего удостоверяющего центра.

11.7. Все Операторы электронных площадок в совокупности обязаны до 01.04.2011 года обеспечить наличие точек выдачи в каждом субъекте Российской Федерации, исходя из следующего:

а) одна точка выдачи, если на территории субъекта Российской Федерации авторизованных до трёх тысячи участников размещения заказа;

б) две точки выдачи, если на территории субъекта Российской Федерации авторизованных от трёх до пяти тысяч участников размещения заказа;

в) три точки, если на территории субъекта Российской Федерации авторизованных от пяти до восьми тысяч участников размещения заказа.

г) четыре точки, если на территории субъекта Российской Федерации авторизованных от восьми до десяти тысяч участников размещения заказа.

д) пять точек, если на территории субъекта Российской Федерации авторизованных от десяти тысяч участников размещения заказа.

Территориальная принадлежность участника размещения заказа определяется по индивидуальному идентификационному номеру налогоплательщика указанному при авторизации.

11.8 За невыполнение либо ненадлежащее выполнение обязательства, предусмотренного в пункте 11.6 настоящего Регламента, Контролирующий орган взыскивает с Оператора электронной площадки неустойку в размере 500 тысяч рублей за каждый календарный месяц просрочки выполнения указанного обязательства.

11.9 За невыполнение либо ненадлежащее выполнение обязательства, предусмотренного в пункте 11.7. настоящего Регламента, Контролирующий орган взыскивает с каждого Оператора электронной площадки неустойку в размере 500 тысяч рублей за каждый календарный месяц просрочки выполнения указанного обязательства.

11.10 В случае нарушения требований настоящего Регламента, Контролирующий орган вправе наложить штраф на виновного Оператора в размере 200 тысяч рублей. кроме пунктов 11.8, 11.9.

11.11. Взыскание неустойки за неисполнение либо ненадлежащее исполнение обязательства, предусмотренного пунктах 11.8, 11.9, 11.10 настоящего Регламента, осуществляется по требованию Контролирующего органа за счёт обеспечения оператора, предоставленного в соответствии с Техническим заданием на функционирование электронных площадок в целях проведения открытых аукционов в электронной форме операторов электронных площадок, в одностороннем внесудебном порядке.

11.12. При взыскании с Оператора неустоек и административных штрафов за неисполнение либо ненадлежащее исполнение обязательств Авторизованным удостоверяющим центром по изготовлению, выдаче и использованию сертификатов ключей подписи участникам размещения заказа, осуществляется по требованию Контролирующего органа за счёт обеспечения Оператора, предоставленного в соответствии с Техническим заданием на функционирование электронных площадок в целях проведения открытых аукционов в электронной форме операторов электронных площадок, в одностороннем внесудебном порядке, Оператор имеет право регрессного требования к Авторизованному удостоверяющему центру в размере уплаченных неустоек и штрафов.

11.13. Неустойки, подлежащие уплате оператором электронной площадки в соответствии с настоящим Регламентом, зачисляются на счет, указанный Контролирующим органом.

Приложение № 1
к Регламенту взаимодействия авторизованных удостоверяющих центров
и электронных площадок, отобранных для проведения открытых аукционов
в электронной форме в соответствии с главой 3.1
Федерального закона от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров,
выполнение работ, оказание услуг для государственных и муниципальных нужд»

ТРЕБОВАНИЯ
к авторизации удостоверяющего центра, осуществляющего изготовление и управление сертификатами ключей подписей для участников размещения заказа на электронных площадках

I. Общие положения

1.1. Настоящий документ устанавливает требования к удостоверяющим центрам, осуществляющим деятельность удостоверяющего центра в отношении участников размещения заказа на электронных площадках.

1.2. После получение статуса Авторизованный удостоверяющий центр должен обеспечить соблюдение указанных требований на протяжении всего периода оказания услуг по осуществление деятельности удостоверяющего центра в отношении участников размещения заказа на электронных площадках.

1.3. К данному документу применимы термины и их определения, приведенные в настоящем Регламенте, а также:

– ключевая информация - закрытые и открытые ключи, предназначенные для формирования (проверки) электронной цифровой подписи, действующие в течение определенного срока;

– ключевой носитель - физический носитель определенной структуры, предназначенный для хранения ключевой информации, а при необходимости - контрольной, служебной и технологической информации.

– ключевой документ – ключевой носитель, содержащий ключевую информацию.

I. Нормативно-правовые требования к удостоверяющему центру

1.1. Удостоверяющий центр должен иметь лицензии ФСБ России на следующие виды деятельности:

– на распространение шифровальных (криптографических) средств;

– на техническое обслуживание шифровальных (криптографических) средств;

– на оказание услуг в области шифрования информации.

1.2. Сертификаты ключей подписей уполномоченного лица удостоверяющего центра, с использованием которых формируются сертификаты ключей подписей участников размещения заказа и списки отозванных сертификатов, должны быть занесены в единый государственный

реестр сертификатов ключей подписей удостоверяющих центров (www.reestr-pki.ru).

При изготовлении нового сертификата ключа подписи уполномоченного лица удостоверяющего центра (по причине плановой либо внеплановой смены ключей) удостоверяющий центр обязан в месячный срок обеспечить занесение нового сертификата ключа подписи в Единый государственный реестр сертификатов ключей подписей удостоверяющих центров.

1.3. Удостоверяющий центр должен осуществлять деятельность удостоверяющего центра исключительно в рамках соответствующего договора (регламента) с участником размещения заказа. Данный договор (регламент) должен устанавливать:

– порядок формирования ключей подписей и изготовления сертификата ключа подписи;

– порядок аннулирования (отзыва) сертификата ключа подписи;

– порядок приостановления (возобновления) действия сертификата ключа подписи;

– момент времени аннулирования (отзыва), приостановления (возобновления) действия сертификата ключа подписи;

– порядок проведения экспертной процедуры по подтверждению подлинности электронной цифровой подписи в электронном документе.

II. Технические требования по осуществлению деятельности удостоверяющего центра

2.1. Требования к средствам автоматизации деятельности удостоверяющего центра

2.1.1. Средства автоматизации деятельности удостоверяющего центра должны быть сертифицированы ФСБ России (система сертификации – РОСС RU.0001.030001) по классу обеспечения информационной безопасности не ниже КС2.

2.1.2. Средство автоматизации деятельности удостоверяющего центра должно изготавливать сертификаты открытых ключей стандарта X.509v3 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

2.1.3. Средство автоматизации деятельности удостоверяющего центра должно изготавливать списки отозванных сертификатов стандарта X.509v2 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

2.2. Требования к используемым средствам электронной цифровой подписи (средствам криптографической защиты информации)

2.2.1. Используемые удостоверяющим центром средства электронной цифровой подписи (средства криптографической защиты информации) должны быть сертифицированы ФСБ России (система сертификации – РОСС RU.0001.030001) по классу обеспечения информационной безопасности не ниже КС2.

2.2.2. Используемое средство электронной цифровой подписи (средство криптографической защиты информации) должно реализовывать ГОСТ Р 34.10-2001, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94 и ГОСТ 28147-89 с учетом RFC 4491 "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms".

2.2.3. Используемое средство электронной цифровой подписи (средство криптографической защиты информации) должно поддерживать формат криптографических сообщений согласно RFC 3852 "Cryptographic Message Syntax (CMS)" с учетом RFC 4490 "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)"

2.2.4. В состав средства электронной цифровой подписи (средства криптографической защиты информации) должно входить средство сетевой аутентификации, обеспечивающее реализацию сетевого протокола SSL/TLS (Secure Sockets Layer/Transport Layer Security) с использованием российских криптографических стандартов электронной цифровой подписи, подсчета хеш-функции и шифрования. Сертификат соответствия ФСБ России должен распространяться на указанное средство сетевой аутентификации.

2.3. Требования к информированию операторов электронных площадок и участников размещения заказа о статусе сертификатов ключей подписей с использованием списков отозванных сертификатов

2.3.1. Удостоверяющий центр должен обеспечить круглосуточное информирование операторов электронных площадок и участников размещения заказа о статусе сертификатов ключей подписей, изданных удостоверяющим центром с использованием списков отозванных сертификатов.

2.3.2. Данное информирование должно осуществляться посредством ежедневного формирования и публикации выписки из реестра удостоверяющего центра, включающего серийные номера сертификатов ключей подписей, которые отозваны или действие которых приостановлено на момент формирования данной выписки (формировать и публиковать списки отозванных сертификатов). При этом, в случае отзыва сертификата ключа подписи участника размещения заказа, удостоверяющий центр обязан опубликовать в точках распространения списков отозванных сертификатов и направить Уполномоченному оператору обновлённый список отозванных сертификатов в течении тридцати минут после поступления в Авторизованный удостоверяющий центр от участника размещения заказа заявления на отзыв сертификата ключа подписи.

2.3.3. Период действия списка отозванных сертификатов не должен превышать 1(одного) дня.

2.3.4. Списки отозванных сертификатов должны размещаться на сетевых ресурсах, круглосуточно доступных операторам электронных площадок и участникам размещения заказа.

2.3.5. Удостоверяющий центр должен обеспечить наличие актуального списка отозванных сертификатов на указанных сетевых ресурсах в течение всех суток. При этом актуальным списком отозванных сертификатов на определенный момент времени считается список отозванных сертификатов, для которого данный момент времени лежит внутри временного интервала, определяемого значениями полей «ThisUpdate» и «NextUpdate» списка отозванных сертификатов.

2.3.6. Адреса сетевых ресурсов размещения списков отозванных сертификатов должны заноситься в издаваемые удостоверяющим центром сертификаты ключей подписей в расширение «Точки распространения списков отозванных сертификатов» (объектный идентификатор расширения сертификата – 2.5.29.31).

2.3.7. Удостоверяющий центр должен обеспечить публикацию списков отозванных сертификатов как минимум в двух сетевых ресурсах (точках распространения). При этом доступ к указанным сетевым ресурсам должен обеспечиваться по различным каналам связи (разнесение сетевых ресурсов публикации списков отозванных сертификатов по различным интернет-провайдерам).

2.3.8. Удостоверяющий центр должен иметь систему оперативного оповещения ответственных сотрудников уполномоченного оператора или организации, указанной в п. 3.16. настоящего Регламента, о невозможности публикации списков отозванных сертификатов в указанных сетевых ресурсах. При возникновении данной ситуации удостоверяющий центр обязан обеспечить актуальность списков отозванных сертификатов всеми возможными способами, в том числе и посредством ручного переноса файлов списков отозванных сертификатов с места их издания в место публикации на указанных сетевых ресурсах.

III. Требования к порядку формирования ключевых документов, изготовления и управления сертификатами ключей подписей

3.1. Удостоверяющий центр должен обеспечить формирование закрытых ключей подписей на сертифицированных по требованиям безопасности информационных технологий ключевых носителях, предназначенных для хранения ключевой информации (смарт-карты, usb-исполнение смарт-карты («токен»)).

3.2. Данные ключевые носители должны поддерживаться применяемым средством электронной цифровой подписи (средством криптографической защиты информации).

3.3. Формирование закрытых ключей должно осуществляться средством электронной цифровой подписи (средством криптографической защиты информации) непосредственно на используемый ключевой носитель, без

сохранения сформированной ключевой информации Удостоверяющем центром на каком-либо ином носителе.

3.4. Формирование закрытого ключа и изготовление сертификата ключа подписи должно быть осуществлено на основании заявления участника размещения заказа в бумажной форме (Приложение № 3 настоящего Регламента). Заявление должно иметь собственноручную подпись владельца сертификата.

Для изготовления сертификата ключа подписи для участия в электронном аукционе участник размещения заказа предоставляет в Авторизованный удостоверяющий центр следующие документы:

а) для юридических лиц и индивидуальных предпринимателей:

- нотариально заверенную доверенность представителя юридического лица, уполномоченного на получение сертификата ключа подписи участника размещения заказа, в случае, если интересы организации представляет не единоличный исполнительный орган (Приложение № 3 настоящего Регламента);
- оригинал или нотариально заверенную копию выписки из ЕГРЮЛ (для индивидуального предпринимателя – ЕГРИП), полученную не позднее чем за месяц до представления;

б) для физических лиц:

- копию документа, удостоверяющего личность в соответствии с законодательством Российской Федерации;
- нотариально заверенную копию свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации.

3.5. Удостоверяющий центр обязан обеспечить формирование закрытого ключа и изготовление сертификата ключа подписи при личном прибытии его владельца либо полномочного представителя владельца в Точку выдачи. Полномочия представителя владельца должны быть подтверждены доверенность или иным документом, подтверждающим его полномочия на подачу заявления на изготовление сертификата ключа подписи.

При изготовлении сертификата ключа подписи удостоверяющим центром должны быть оформлены в форме документов на бумажном носителе два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями владельца сертификата ключа подписи, и ответственного лица удостоверяющего центра, уполномоченного на осуществление указанного действия, а также печатью удостоверяющего центра.

3.6. Аннулирование (отзыв), приостановление и возобновление действия сертификата ключа подписи должны быть осуществлены на основании заявления участника размещения заказа в бумажной форме, которое должно содержать серийный номер сертификата и идентификационные данные его владельца. Минимальный срок приостановления действия сертификата ключа подписи составляет пятнадцать дней. Возобновление действия сертификата

ключа подписи может быть осуществлено только в период времени, на который действие сертификата ключа подписи было приостановлено.

3.7. Заявительные документы на изготовление, аннулирование (отзыв), приостановление и возобновление сертификатов ключей подписей, а также документы, подтверждающие права того или иного лица на выполнение определенных действий, должны оформляться в соответствии с формами документов, приведенными в Приложении № 3 к настоящему Регламенту.

3.8. В случае изменения статуса сертификата ключа подписи участника размещения заказа удостоверяющий центр обязан обеспечить информирование операторов электронных площадок и участников размещения заказа путём публикации нового списка отозванных сертификатов не позднее тридцати минут с момента изменения статуса сертификата.

IV. Требования к ключевым документам и сертификатам ключей подписей, формируемых удостоверяющим центром

4.1. Требования к срокам действия ключевых документов и сертификатам ключей подписей

4.1.1. Срок действия закрытого ключа подписи участника размещения заказа не должен превышать максимальный срок действия закрытого ключа, установленный используемым средством электронной цифровой подписи (средством криптографической защиты информации).

4.1.2. Срок действия сертификата ключа подписи не должен превышать максимальный срок действия сертификата ключа подписи, установленный используемым средством электронной цифровой подписи (средством криптографической защиты информации).

4.1.3. Информация о сроке действия закрытого ключа подписи и сроке действия сертификата ключа подписи должна заноситься в издаваемые удостоверяющем центром сертификаты ключей подписей.

4.1.4. Удостоверяющий центр обязан обеспечить информирование участников размещения заказа о скором истечении срока действия их закрытых ключей. Первое уведомление должно быть направлено не позднее тридцати дней до окончания срока действия закрытого ключа, второе уведомление – не позднее четырнадцати дней до окончания срока действия закрытого ключа.

4.2. Требования к составу сертификата ключа подписи участника размещения заказа

4.2.1. Сертификат ключа подписи, издаваемый удостоверяющим центром для участника размещения заказа должен соответствовать стандарту X.509v3 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

4.2.2. Сертификат ключа подписи участника размещения заказа должен соответствовать следующей структуре:

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CN = Псевдоним уполномоченного лица Удостоверяющего центра O = Организация OU = Подразделение L = Город S = Субъект федерации C = Страна/Регион = RU E = Электронная почта
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = ФИО владельца сертификата T = Должность (для юридических лиц) O = Организация (для юридических лиц) OU = Подразделение (для юридических лиц) L = Город S = Субъект федерации C = Страна/Регион = RU E = Электронная почта UnsructuredName (UN) = ИНН/КПП/ОГРН организации (для юридических лиц) и ИНН (для физических лиц и индивидуальных предпринимателей) В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 5280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Проверка подлинности клиента (OID 1.3.6.1.5.5.7.3.2) Защищенная электронная почта (OID 1.3.6.1.5.5.7.3.4) Использование на электронных площадок отобранных для проведения аукционах в электронной форме(OID 1.2.643.6.3.1.1) Области использования согласно заявлению клиента: . Тип участника (один вариант из списка) 1. Юридическое лицо(OID 1.2.643.6.3.1.2.1) 2. Физическое лицо(OID 1.2.643.6.3.1.2.2) 3. Индивидуальный предприниматель(OID 1.2.643.6.3.1.2.3) . Тип организации: 1. Участник размещения заказа(OID 1.2.643.6.3.1.3.1) . Полномочия (множественный выбор): 1. Администратор организации(OID 1.2.643.6.3.1.4.1) 2. Уполномоченный специалист(OID 1.2.643.6.3.1.4.2) 3. Специалист с правом подписи контракта (OID 1.2.643.6.3.1.4.3)

Application Policy	Политика применения	Набор областей использования ключей и сертификатов(Необязательное поле)
Certificate Policies	Политики сертификатов	Набор областей использования ключей и сертификатов
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/Name.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, Name - имя файла списка отозванных сертификатов .
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно, RFC 5280

4.2.3. Поле «Субъект» сертификата ключа подписи, идентифицирующего владельца сертификата ключа подписи, должно содержать следующие компоненты имени:

– компонент «Общее имя» (CN, Common Name), содержащий фамилию, имя, отчество владельца сертификата с разделителями в один пробел (Фамилия Имя Отчество) (обязательное к заполнению);

– компонент «Организация» (O, Organization), содержащий название организации владельца сертификата - только для юридических лиц (обязательное к заполнению);

– компонент «Должность» (T, Title), содержащий название должности владельца сертификата в организации - только для юридических лиц (обязательное к заполнению);

– компонент «Город» (L, Locality), содержащий название населённого пункта, в котором расположена организация владельца сертификата – для юридических лиц; название населенного пункта, в котором зарегистрирован владелец сертификата – для физических лиц (обязательное к заполнению);

– компонент «Область/Край» (S, State), содержащий название региона, в котором расположена организация владельца сертификата – для юридических лиц; название региона, в котором зарегистрирован владелец сертификата – для физических лиц (обязательное к заполнению);

– компонент «Страна/регион» (C, Country), содержащее двухзначный код страны (например, «RU»), в котором расположена организация владельца сертификата – для юридических лиц; двухзначный код страны, в котором зарегистрирован владелец сертификата – для физических лиц (обязательное к заполнению);

– компонент «Электронная почта» (E, EMail), содержащее адрес электронной почты владельца сертификата ключа подписи (обязательное к заполнению);

– компонент «Неструктурированное имя» (UN, Unsructured Name), содержащее INN=ИНН\KPP=КПП\OGRN=ОГРН организации владельца сертификата для юридических лиц и INN=ИНН для физических лиц и индивидуальных предпринимателей (обязательное к заполнению).

4.2.4. В сертификате ключа подписи участника размещения заказа расширение «Улучшенный ключ» (OID 2.5.29.37) должно содержать значения: «Проверка подлинности клиента» (OID 1.3.6.1.5.5.7.3.2), «Защищенная электронная почта» (OID 1.3.6.1.5.5.7.3.4).

4.2.5. В сертификате ключа подписи в расширении «Улучшенный ключ», согласно заявлению участника размещения заказа, содержатся сведения, устанавливающие правомерность использования сертификата ключа подписи на электронных площадках:

Использование на электронных площадок отобранных для проведения аукционах в электронной форме(OID 1.2.643.6.3.1.1)

Тип участника (один вариант из списка)

1. Юридическое лицо (OID 1.2.643.6.3.1.2.1)
2. Физическое лицо (OID 1.2.643.6.3.1.2.2)
3. Индивидуальный предприниматель (OID 1.2.643.6.3.1.2.3)

Тип организации:

1. Участник размещения заказа (OID 1.2.643.6.3.1.3.1)

Полномочия (множественный выбор):

1. Администратор организации (OID 1.2.643.6.3.1.4.1)
2. Уполномоченный специалист (OID 1.2.643.6.3.1.4.2)
3. Специалист с правом подписи контракта(OID 1.2.643.6.3.1.4.3)

4.3. Требования к составу списка отозванных сертификатов, публикуемого удостоверяющим центром

4.3.1. Список отозванных сертификатов, издаваемый удостоверяющим центром должен соответствовать стандарту X.509v2 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

4.3.2. Список отозванных сертификатов должен соответствовать следующей структуре:

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = Псевдоним уполномоченного лица Удостоверяющего центра O = Организация OU = Подразделение L = Город S = Субъект федерации C = Страна/Регион = RU E = Электронная почта
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа

		"2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа уполномоченного лица Удостоверяющего центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата уполномоченного лица Удостоверяющего центра (необязательное поле)
CRLNumber	Номер СОС	Порядковый номер выпущенного СОС

Приложение № 1

к Регламенту получения сертификатов ключей подписи и использования электронной цифровой подписи

ЗАЯВЛЕНИЕ
на прохождение авторизации удостоверяющего центра, претендующего на получение права оказания услуг по изготовлению и управлению сертификатами ключей подписей для участников размещения заказа на электронных площадках

Прошу рассмотреть настоящее заявление на прохождение авторизации удостоверяющего центра с целью предоставления права оказания услуг по изготовлению и управлению сертификатами ключей подписей для участников размещения заказа на электронных площадках.

Реквизиты удостоверяющего центра:
Полное наименование: _____
Юридический адрес: _____
Фактический адрес: _____
Адрес для корреспонденции: _____
Банковские реквизиты (наименование банка, БИК, ИНН, р/с, к/с):
_____
ИНН/КПП: _____/_____
ОГРН: _____
Контактные телефоны, факс, адрес электронной почты:
_____

Руководитель _____ /_____/

М.П. (подпись)

Приложение № 2

к Регламенту получения сертификатов ключей подписи и использования электронной цифровой подписи

ФОРМЫ
заявительных документов, предоставляемых пользователем в авторизованный удостоверяющий центр для изготовления и управления сертификатами ключей подписей

ФОРМА
заявления на изготовление сертификата ключа подписи (для юридических и физических лиц)

Для юридических лиц

_____

(наименование авторизованного

_____

удостоверяющего центра)

Заявление
на изготовление сертификата ключа подписи

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность, фамилия, имя, отчество)

действующего на основании _____

Просит создать закрытый и открытый ключи электронной цифровой подписи и изготовить сертификат ключа подписи уполномоченного представителя

_____

(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении данными:

Title (T)	Должность
CommonName (CN)1	Фамилия, Имя, Отчество*
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	RU
E-Mail (E)	Адрес электронной почты
Неструктурированное имя	INN=ИНН\KPP=КПП\OGRN=ОГРН

Тип участника (один вариант из списка)	ЮЛ, ФЛ, Индивидуальный предприниматель
Тип организации (один вариант из списка)	Участник размещения заказа
Полномочия (множественный выбор)	Администратор организации, Уполномоченный специалист Специалист с правом подписи контракта

Настоящим _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и кода выдан)
соглашается с обработкой своих персональных данных Удостоверяющим центром _____и признает, что персональные данные, заносимые в
(наименование удостоверяющего центра)
сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Руководитель организации _____ _____
(подпись) М.П. (фамилия, инициалы)

«____» _____ 20____ г.

Для физических лиц

_____
(наименование авторизованного
_____
удостоверяющего центра)

Заявление
на изготовление сертификата ключа подписи

_____
(фамилия, имя, отчество)
_____
(номер и серия документа, удостоверяющего личность, когда и кем выдан)

прошу создать закрытый и открытый ключи электронной цифровой подписи и изготовить сертификат ключа подписи с правом участия в качестве участника размещения заказа на электронных площадках, отобранных для проведения открытых аукционов в электронной форме в соответствии с главой 3.1. Федерального закона от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» в соответствии с указанными в настоящем заявлении данными:

CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	RU
E-Mail (E)	Адрес электронной почты
Тип участника (один вариант из списка)	ФЛ, Индивидуальный предприниматель
Тип организации (один вариант из списка)	Участник размещения заказа
Полномочия (множественный выбор)	Администратор организации, Уполномоченный специалист, Специалист с правом подписи контракта

Настоящим _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и кода выдан)
соглашается с обработкой своих персональных данных Удостоверяющим центром _____и признает, что персональные данные, заносимые в
(наименование удостоверяющего центра)
сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

_____ (фамилия, инициалы)
(подпись)
«____» _____ 20____ г.

ФОРМА
доверенности полномочного представителя юридического лица,
наделенного правом участвовать на электронных площадках
с использованием электронной цифровой подписи
(только для юридических лиц)

Доверенность

_____ «_____» _____ 20___ г.

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____
(должность)
_____
(фамилия, имя, отчество)
действующего на основании _____
уполномочивает _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и когда выдан)

выступать в роли Пользователя Удостоверяющего центра _____
(наименование удостоверяющего центра)
с правом участия в качестве участника размещения заказа на электронных площадках, отобранных для проведения открытых аукционов в электронной форме в соответствии с главой 3.1. Федерального закона от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд», а также внести следующие сведения, устанавливающие правомерность использования сертификата ключа подписи его владельцем на электронных площадках:

Тип участника (один вариант из списка)	ЮЛ
Тип организации (один вариант из списка)	Участник размещения заказа
Полномочия (множественный выбор)	Администратор организации, Уполномоченный специалист, Специалист с правом подписи контракта

Настоящая доверенность действительна по «____» _____ 20____г. *

Подпись уполномоченного представителя _____ _____
(Подпись) (Фамилия, инициалы)
подтверждаю.
Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

* Примечание: *- срок действия доверенности должен быть не менее срока действия закрытого ключа, соответствующего изготавливаемому сертификату.

ФОРМА
доверенности, выдаваемая полномочному представителю
юридическим лицом и владельцем сертификата ключа подписи,
на получение за владельца сертификата
ключи подписи и сертификат ключа подписи
(только для юридических лиц)

_____[1]
«_____»[2]

ИНН _____[3] ОКАТО _____[4]
юридический адрес: _____[5]

ДОВЕРЕННОСТЬ

город _____[6]**, _____**[7]
_____[8] «_____»[9], в лице _____[10] _____[11], действующего на основании _____[12], настоящей доверенностью уполномочивает _____[13] _____[14]:

1. Предоставить в Удостоверяющий центр _____[15] «_____»16 документы, необходимые для изготовления сертификата ключа подписи полномочного представителя _____[17] «_____»[18] - Пользователя Удостоверяющего центра _____[19]
_____

[1] Указывается организационно-правовая форма юридического лица согласно учредительным документам (например, открытое акционерное общество)

[2] Указывается полное наименование юридического лица согласно учредительным документам

[3] Указывается ИНН юридического лица

[4] Указывается ОКАТО юридического лица

[5] Указывается юридический адрес юридического лица

[6] Указывается место составления доверенности

[7] Указывается дата составления доверенности (например, «третье июня две тысячи десятого года»)

[8] Указывается организационно-правовая форма юридического лица (например, ООО)

[9] Указывается сокращенное наименование юридического лица согласно учредительным документам

[10] Указывается должность лица, уполномоченного действовать от имени юридического лица (например, генерального директора)

[11] Указывается фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица (например, Петрова Петра Петровича)

[12] Указывается документ (документы) и его реквизиты, на основании которого (которых) указанное лицо уполномочено действовать от имени юридического лица (например, устава, доверенности от №).

[13] Указывается фамилия, имя, отчество доверенного лица

[14] Указывается документ, удостоверяющий личность доверенного лица, и его реквизиты

[15] Указывается организационно-правовая форма (например, ООО) Удостоверяющего центра

[16] Указывается полное наименование Удостоверяющего центра согласно учредительным документам

[17] Указывается организационно-правовая форма (например, ООО) юридического лица

[18] Указывается сокращенное наименование юридического лица согласно учредительным документам

«_____»[20], имеющего право участвовать в качестве участника размещения заказа на Отобранных электронных площадках.

2. Получить сертификат ключа подписи уполномоченного лица Удостоверяющего центра _____[21] «_____»[22]сформированные ключи подписи и сертификат ключа подписи Пользователя Удостоверяющего центра - _____[23]

Доверенность выдана сроком на _____[24] без права передоверия.

_____ _____ (ФИО)
(подпись)
МП

---

[19] Указывается организационно-правовая форма (например, ООО) Удостоверяющего центра

[20] Указывается сокращенное наименование Удостоверяющего центра согласно учредительным документам

[21] Указывается организационно-правовая форма (например, ООО) Удостоверяющего центра

[22] Указывается сокращенное наименование Удостоверяющего центра согласно учредительным документам

[23] Указывается фамилия, имя, отчество Пользователя Удостоверяющего центра – участника размещения заказа

[24] Указывается срок, на который выдается доверенность, который согласно действующему законодательству не может превышать трех лет.

ФОРМА
заявления на аннулирование (отзыв) сертификата ключа подписи
(для юридических и физических лиц)

Для юридических лиц

_____
(наименование авторизованного
_____
удостоверяющего центра)

Заявление
на аннулирование (отзыв) сертификата ключа подписи

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

в лице _____,
(должность)
_____,
(фамилия, имя, отчество)

действующего на основании _____

в связи с _____
(причина отзыва сертификата)

Просит аннулировать (отозвать) сертификат ключа подписи своего уполномоченного представителя:
_____
(фамилия, имя, отчество)

содержащий следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
SurName (SN)	Фамилия, Имя, Отчество
Неструктурированное имя	KPP=ИНН\KPP=КПП\OGRN=ОГРН (ИНН организации \ КПП организации\ОГРНфизического лица, на которого выдается сертификат)
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество (псевдоним)
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
OrganizationUnit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Владелец сертификата ключа подписи _____ /Фамилия И.О./
«____» _____ 20____ г.

Должность и Ф.И.О. уполномоченного лица организации
Подпись уполномоченного лица организации, дата подписания заявления
Печать организации

Для физических лиц

_____
(наименование авторизованного
_____
удостоверяющего центра)

Заявление
на аннулирование (отзыв) сертификата ключа подписи

Я, _____
(фамилия, имя, отчество)
в связи с _____
(причина отзыва сертификата)
прошу аннулировать (отозвать) сертификат ключа подписи, содержащий следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

_____ /Фамилия И.О./
(подпись)
«____» _____ 20____ г.

ФОРМА
заявления на приостановление действия сертификата ключа подписи
(для юридических и физических лиц)

Для юридических лиц

_____
(наименование авторизованного
_____
удостоверяющего центра)

Заявление
на приостановление действия сертификата ключа подписи

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

в лице _____,
(должность)
_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит приостановить действие сертификата ключа подписи своего уполномоченного представителя:

_____
(фамилия, имя, отчество)

содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
SurName (SN)	Фамилия, Имя, Отчество
Неструктурированное имя	KPP=ИНН\KPP=КПП\OGRN=ОГРН (ИНН организации \ КПП организации\ОГРНфизического лица, на которого выдается сертификат)
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество (псевдоним)
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
OrganizationUnit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

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

Владелец сертификата ключа подписи _____ /Фамилия И.О./
«____» _____ 20____ г.

Должность и Ф.И.О. уполномоченного лица организации
Подпись уполномоченного лица организации, дата подписания заявления
Печать организации

Для физических лиц

_____
(наименование авторизованного
_____
удостоверяющего центра)

Заявление
на приостановление действия сертификата ключа подписи

Я, _____
(фамилия, имя, отчество)
прошу приостановить действие сертификата ключа подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

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

_____ /Фамилия И.О./
(подпись)
«____» _____ 20____ г.

ФОРМА
заявления на возобновление действия сертификата ключа подписи
(для юридических и индивидуальных предпринимателей)

Для юридических лиц

_____
(наименование авторизованного
_____
удостоверяющего центра)

Заявление
на возобновление действия сертификата ключа подписи

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

в лице _____,
(должность)
_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие сертификата ключа подписи своего уполномоченного представителя:

_____
(фамилия, имя, отчество)

содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
SurName (SN)	Фамилия, Имя, Отчество
Неструктурированное имя	KPP=ИНН\KPP=КПП\OGRN=ОГРН (ИНН организации \ КПП организации\ОГРНфизического лица, на которого выдается сертификат)
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество (псевдоним)
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
OrganizationUnit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Владелец сертификата ключа подписи _____ /Фамилия И.О./
«____» _____ 20____ г.

Должность и Ф.И.О. уполномоченного лица организации
Подпись уполномоченного лица организации, дата подписания заявления
Печать организации

Для физических лиц

_____
(наименование авторизованного
_____
удостоверяющего центра)

Заявление
на возобновление действия сертификата ключа подписи

Я, _____
(фамилия, имя, отчество)
прошу возобновить действие сертификата ключа подписи, содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

_____ /Фамилия И.О./
(подпись)
«____» _____ 20____ г.

Приложение № 3

к Регламенту получения сертификатов ключей подписи и использования электронной цифровой подписи

СОГЛАШЕНИЕ

о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров

Термины и определения

Оператор электронной площадки (оператор) – оператор электронной площадки, отобранной для проведения открытых аукционов в электронной форме в соответствии с главой 3.1. Федерального закона от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

Авторизованный удостоверяющий центр – юридическое лицо, осуществляющее выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом от 10.01.2002г. № 1-ФЗ «Об электронной цифровой подписи», и заключивший договор авторизации с одним из операторов электронной площадки.

К настоящему Соглашению применимы термины и их определения, приведенные в Регламенте получения сертификатов ключей подписей и использования электронной цифровой подписи (далее - Регламент).

Статус СОГЛАШЕНИЯ

Настоящее Соглашение является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

Сторонами настоящего Соглашения являются присоединившиеся к Соглашению Операторы электронных площадок и Авторизованные удостоверяющие центры.

Общие положения

Присоединение сторон к Соглашению

Присоединение к настоящему Соглашению сторон осуществляется в следующем порядке:
1. Присоединение Операторов электронных площадок;
2. Присоединение Авторизованных удостоверяющих центров.

Присоединение к настоящему Соглашению Операторов электронных площадок и Авторизованных удостоверяющих центров осуществляется путем подписания заявления о присоединении к настоящему Соглашению.

Операторы электронных площадок подписывают заявление о присоединении к настоящему Соглашению согласно форме, приведенной в Приложении №1 к настоящему Соглашению.

Авторизованные удостоверяющие центры подписывают заявление о присоединении к настоящему Соглашению согласно форме, приведенной в Приложении №2 к настоящему Соглашению.

Настоящее соглашение действительно для каждой из сторон только в случае если они являются Оператором электронной площадке или Авторизованным удостоверяющем центром.

С момента подписания указанного заявления о присоединении Оператор электронной площадки и Авторизованный удостоверяющий центр считаются присоединившимися к настоящему Соглашению и становятся Сторонами настоящего Соглашения.

Факт присоединения Стороны к Соглашению является полным принятием им условий настоящего Соглашения.

После присоединения к Соглашению стороны, присоединившиеся к нему, вступают в соответствующие договорные отношения на неопределённый срок.

Заявление о присоединение к настоящему Соглашению может быть подано организацией до получения такой оргниазции статуса Авторизованного удостоверяющего центра. В этом случае правовые последствия связанные с присоединением к настоящему соглашению наступают для такой оргниазации с момента получения последней статуса Авторизованного удостоверяющего центра.

Права и обязанности сторон

Права и обязанности присоединившегося к Соглашению Операторов:

Оператор, присоединившийся к настоящему Соглашению, обязан обеспечить на своей электронной торговой площадке использование сертификатов ключей подписей участников размещения заказа, издаваемых Авторизованными удостоверяющими центрами, присоединившимися к настоящему Соглашению.

Оператор, присоединившийся к настоящему Соглашению обязан осуществлять проверку подлинности сертификатов открытых ключей электронных цифровых подписей участников размещения заказа согласно Регламенту.

Права и обязанности присоединившегося к Соглашению Авторизованного удостоверяющего центра:

Авторизованный удостоверяющий центр на момент присоединения к настоящему Соглашению обязан обеспечить технологическую совместимость издаваемых ключей подписей и сертификатов ключей подписей и программно-аппаратных комплексов Операторов электронных площадок, присоединившихся к настоящему Соглашению.

Авторизованный удостоверяющий центр обязан обеспечить изготовление и управление сертификатами ключей подписей участников размещения заказа в соответствии с Регламентом.

Авторизованный удостоверяющий центр обязан обеспечить достоверность сведений, заносимых в изготавливаемые сертификаты ключей подписей участников размещения заказа.

Авторизованный удостоверяющий центр обязан обеспечить публикацию списков отозванных сертификатов и предоставление корневого сертификата в соответствии с Регламентом.

Ответственность сторон

В случае неисполнения либо ненадлежащего исполнения обязательств по настоящему Соглашению Стороны несут ответственность, установленную Гражданским кодексом Российской Федерации и иными правовыми актами Российской Федерации.

Разрешение споров

При рассмотрении спорных вопросов, связанных с настоящим Соглашением, Стороны, присоединившиеся к нему, будут руководствоваться действующим законодательством Российской Федерации.

Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

Спорные вопросы между сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде по месту нахождения Оператора электронной площадки, если одной из сторон спора является Оператор электронной площадки.

Список приложений

Приложение № 1. Образец заявления о присоединении к Соглашению о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров (для Оператора электронной площадки).

Приложение № 2. Образец Заявления о присоединении к Соглашению о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров (для Авторизованного удостоверяющего центра).

Приложение № 1
к Соглашению о взаимодействии операторов электронных площадок
и авторизованных удостоверяющих центров

ЗАЯВЛЕНИЕ О ПРИСОЕДИНЕНИИ
к Соглашению о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров

_____
(Оператор электронной площадки)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяется к Соглашению о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров на правах Оператора электронной площадки. С Соглашением о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров ознакомлен и обязуюсь соблюдать все положения указанного документа.

Генеральный директор _____/_____/
«___» _____ 20___г.
М.П.

Приложение № 2
к Соглашению о взаимодействии операторов электронных площадок
и авторизованных удостоверяющих центров

ЗАЯВЛЕНИЕ О ПРИСОЕДИНЕНИИ
к Соглашению о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров

_____
(Авторизованный удостоверяющий центр)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяется к Соглашению о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров на правах Авторизованного удостоверяющего центра.
С Соглашением о взаимодействии операторов электронных площадок и авторизованных удостоверяющих центров ознакомлен и обязуюсь соблюдать все положения указанного документа.

Генеральный директор _____/_____/
«___» _____ 20___г.
М.П.