

Утверждаю

Генеральный директор

АО «Центр развития экономики»

Д.А. Патрунин



**РЕГЛАМЕНТ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО
ДОКУМЕНТООБОРОТА И ИСПОЛЬЗОВАНИЯ
ЭЛЕКТРОННОЙ ПОДПИСИ
В СИСТЕМЕ B2B-CENTER**

АО «ЦЕНТР РАЗВИТИЯ ЭКОНОМИКИ»

Оглавление

РЕГЛАМЕНТ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В СИСТЕМЕ B2B-CENTER.....	1
1. Общие положения.....	3
2. Термины и определения	4
3. Субъекты регламента	6
4. Общий порядок подключения к системе ЭДО	7
5. Использование простой электронной подписи.....	8
5.1. Общие положения	8
5.2. Правила создания и выдачи ключей.....	8
6. Использование усиленной электронной подписи	10
6.1. Удостоверяющие центры и сертификаты ключей проверки ЭП.....	10
6.2. Средства электронной подписи	11
6.3. Формирование и проверка усиленной электронной подписи	11
6.4. Применение усиленной электронной подписи	12
7. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью.....	15
8. Порядок разрешения конфликтных ситуаций	16
8.1. Общие Положения.....	16
8.2. Документы, предоставляемые инициатором	16
8.3. Порядок работы согласительной комиссии	17
8.4. Оформление результатов работы согласительной комиссии	17
9. Разграничение ответственности	18
10. Прочие условия	19
Приложения	20
Приложение №1	20

1. Общие положения

1. Настоящий Регламент организации электронного документооборота и использования электронной подписи (далее – Регламент) определяет:

- принципы взаимодействия пользователей Системы электронных торгов B2B-Center, расположенной в сети Интернет на сервере по адресу <http://www.b2b-center.ru/> (далее – ЭТП);
- порядок использования электронной подписи в информационной Системе электронного документооборота (Системе ЭДО) Системы B2B-Center;
- правовые условия, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной.

2. Регламент разработан в соответствии с Федеральным законом № 63-ФЗ «Об электронной подписи» от 06.04.2011 г.

3. Регламент размещен (опубликован) в сети Интернет на сервере по адресу: [http://www.b2b-center.ru/help/Регламент организаци... подписи](http://www.b2b-center.ru/help/Регламент_организации_электронного_документооборота_и_использования_электронной_подписи).

4. Регламент не определяет порядок получения сертификатов ключей проверки электронной подписи Участниками ЭТП. Данный порядок определяется договорами, правилами и иными нормативными документами между Участником ЭТП и третьей стороной (Удостоверяющим центром, поставщиком средств электронной подписи), осуществляющей функции по созданию и выдаче сертификатов ключей проверки электронной подписи.

5. Требования к программно-аппаратным средствам Участника ЭТП, необходимым для работы в Системе ЭДО, размещены в сети Интернет на сервере по адресу: <http://www.b2b-center.ru/requirements.html>.

6. Регламент может включать в себя дополнения и приложения, раскрывающие и детализирующие различные положения организации электронного документооборота и использования электронной подписи. Дополнения, приложения к Регламенту, публикуемые на ЭТП, являются неотъемлемой частью Регламента.

7. Требования к сертификатам ключей проверки электронной подписи, используемым в Системе ЭДО, приведены в Приложении №1 Регламента.

8. Субъект Регламента признает Регламент полностью, без изъятий, безусловно и безоговорочно, присоединяется к нему и никогда, ни при каких условиях не будет ссылаться в оправдание своих действий на незнание или непонимание Регламента.

9. Исключительное право на внесение изменений и дополнений в Регламент в порядке, изложенном в Регламенте, имеет Администратор ЭДО.

2. Термины и определения

Для целей Регламента используются следующие основные понятия:

- **Электронная торговая площадка (ЭТП)** – Система электронных торгов B2B-Center, расположенная в сети Интернет на сервере по адресу <http://www.b2b-center.ru/> и являющаяся корпоративной информационной системой, порядок использования электронной подписи в которой устанавливается Администратором ЭДО.
- **Оператор ЭТП** – Акционерное общество «Центр развития экономики», обеспечивающее эксплуатацию, поддержку и сопровождение ЭТП.
- **Администратор ЭДО** – Акционерное общество «Центр электронных расчетов и программ финансирования», обеспечивающее функционирование Системы ЭДО на ЭТП.
- **Участник ЭТП** – физическое или юридическое лицо, индивидуальный предприниматель, получивший в порядке, установленном Оператором ЭТП, право использования ЭТП и совершения действий (операций) в рамках ЭТП, в том числе заключивший соответствующий договор с Оператором ЭТП.
- **Пользователь ЭТП** – лицо, являющееся представителем (сотрудником) Участника ЭТП (собственно Участником ЭТП в случае физического лица) и наделенное надлежащими полномочиями по совершению действий (операций) в рамках ЭТП.
- **Электронная подпись (ЭП)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
- **Электронный документ** – электронное сообщение, подписанное электронной подписью и способное быть преобразованным средствами ЭТП в форму, пригодную для однозначного восприятия его содержания. Электронное сообщение – информация, представленная в электронной форме, переданная или полученная пользователем ЭТП, представляющая собой совокупность структурированных данных, и позволяющая обеспечить ее обработку программно-аппаратным обеспечением ЭТП.
- **Простая электронная подпись** – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
- **Усиленная электронная подпись** – электронная подпись, которая:
 - получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
 - позволяет определить лицо, подписавшее документ;
 - позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
 - создается с использованием средств электронной подписи.

Различаются усиленная неквалифицированная электронная подпись (неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (квалифицированная электронная подпись).

- **Владелец сертификата ключа проверки электронной подписи** – лицо, являющееся уполномоченным представителем Участника ЭТП, которому Удостоверяющим центром выдан сертификат ключа проверки электронной подписи.
- **Ключ проверки электронной подписи (открытый ключ ЭП)** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи, предназначенная для проверки подлинности электронной подписи.
- **Ключ электронной подписи (закрытый ключ ЭП)** - уникальная последовательность символов, предназначенная для создания электронной подписи.
- **Пользователь электронной подписи** – пользователь ЭТП, обладающий правами на использование функциональности электронной подписи.
- **Сертификат ключа проверки подписи (сертификат ключа, СКП)** – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя ключ проверки подписи, или документ на бумажном носителе, выданные Удостоверяющим центром и подтверждающие принадлежность ключа проверки подписи владельцу сертификата ключа проверки подписи.
- **Квалифицированный сертификат ключа проверки подписи (квалифицированный сертификат, квалифицированный СКП)** – сертификат ключа проверки подписи, выданный аккредитованным Удостоверяющим центром, т.е. Удостоверяющим центром, признанным уполномоченным федеральным органом соответствующим требованиям Федерального закона от 06.04.2011 г. № 63-ФЗ.
- **Система электронного документооборота (Система ЭДО B2B-Center)** – совокупность программно-аппаратных средств на стороне Оператора ЭДО и на стороне (рабочих местах) Участников ЭТП, позволяющая осуществлять безопасный, защищенный от третьих лиц обмен электронными документами с использованием электронных подписей на ЭТП в Системе электронных торгов B2B-Center. Система ЭДО B2B-Center является частью Системы электронных торгов B2B-Center.
Подключение пользователя ЭТП к Системе ЭДО означает необходимость получения этим пользователем доступа к функционалу электронной подписи.
- **Удостоверяющий центр** – юридическое лицо или индивидуальный предприниматель, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, по распространению средств электронной подписи, а также иные функции, связанные с использованием электронной подписи, предусмотренные действующим законодательством.
- **Уполномоченное лицо Удостоверяющего центра** - физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром надлежащими полномочиями по подписанию от лица Удостоверяющего центра электронной подписью Удостоверяющего центра сертификатов ключей проверки подписей и списков отозванных сертификатов.
- **Подключенный удостоверяющий центр** – Удостоверяющий центр, информация о корневых сертификатах и точках распространения списков отозванных сертификатов которого внесена в Систему ЭДО B2B-Center.
- **Юрисдикция** – сфера компетенции органов государственной власти и действия норм национального законодательства.

3. Субъекты регламента

1. Субъектами настоящего Регламента являются:

- Оператор ЭТП, выступающий в лице ответственных сотрудников организации;
- Администратор ЭДО, выступающий в лице ответственных сотрудников организации;
- Участники ЭТП, выступающие в лице пользователей ЭТП: владельцев сертификатов ключей проверки подписей и пользователей электронной подписи;
- Удостоверяющие центры, выступающие в лице уполномоченных лиц.

4. Общий порядок подключения к системе ЭДО

1. Администратор ЭДО размещает на ЭТП информацию, необходимую для подключения к Системе ЭДО B2B-Center.
2. Администратор ЭДО предоставляет Участникам ЭТП следующую инфраструктуру Системы ЭДО B2B-Center для получения и обслуживания электронной подписи:
 - Справочную информацию и документы, необходимые для получения электронной подписи, настройки средств электронной подписи, установки сертификата ключа проверки электронной подписи на рабочем месте Участника ЭТП (пользователя электронной подписи) и иную дополнительную информацию;
 - Функционал проверки работоспособности средств электронной подписи, установленных на стороне (рабочем месте) Участника ЭТП (пользователя электронной подписи);
 - Перечень подключенных удостоверяющих центров и их текущих статусов;
 - Функционал регистрации Участниками ЭТП сертификатов ключей проверки подписей, полученных в удостоверяющих центрах, подключенных к Системе ЭДО B2B-Center;
 - Функционал проверки простой электронной подписи Пользователями ЭТП;
 - Функционал создания и выдачи ключей простой электронной подписи Участникам ЭТП.
3. Участник ЭТП изучает информацию, необходимую для подключения к Системе ЭДО B2B-Center, и принимает решение о подключении к Системе ЭДО B2B-Center.
 - 3.1. Участник ЭТП при наличии действующего сертификата ключа проверки электронной подписи, удовлетворяющего требованиям по использованию в Системе ЭДО B2B-Center, направляет Администратору ЭДО заявку на регистрацию сертификата ключа проверки электронной подписи.
 - 3.2. Участник ЭТП при отсутствии сертификата ключа проверки электронной подписи, удовлетворяющего требованиям по использованию в Системе ЭДО B2B-Center, направляет Администратору ЭДО заявку на получение простой или усиленной электронной подписи. В случае получения усиленной электронной подписи Участник ЭТП направляет Администратору ЭДО заявку на регистрацию сертификата ключа проверки электронной подписи.
4. Администратор ЭДО рассматривает заявку Участника ЭТП на получение простой электронной подписи. По результату обработки заявки Участник ЭТП получает доступ к функционалу простой электронной подписи или заявка отклоняется.
 - 4.1. Администратор ЭДО рассматривает заявку Участника ЭТП на получение усиленной электронной подписи и направляет в подключенный аккредитованный удостоверяющий центр для оформления и выдачи сертификата и ключа квалифицированной усиленной электронной подписи.
5. Администратор ЭДО рассматривает полученную заявку на регистрацию сертификата ключа проверки усиленной электронной подписи и регистрирует сертификат для пользователя электронной подписи Участника ЭТП либо отклоняет заявку. Основанием для отклонения заявки служит несоответствие информации, содержащейся в сертификате, информации о зарегистрированном Участнике ЭТП и пользователе электронной подписи.

5. Использование простой электронной подписи

5.1. Общие положения

1. Настоящие правила устанавливают порядок использования простой электронной подписи пользователями ЭТП.
2. Ключом простой электронной подписи является сочетание двух элементов – идентификатора и ПИН-кода ключа. Идентификатором является логин и пароль пользователя на ЭТП, а ПИН-кодом ключа – последовательность символов, созданная в соответствии с настоящими Правилами.
3. Использование пользователями ЭТП простой электронной подписи допускается, если федеральными законами или иными нормативными правовыми актами не установлено использование в этих целях иного вида электронной подписи.
4. Для использования простой электронной подписи пользователь ЭТП должен подать заявку на подключение к функциональности простой электронной подписи. Заявка на подключение к функциональности простой электронной подписи подается заявителем в электронном виде посредством ЭТП и рассматривается Администратором ЭДО. По результату рассмотрения поданной заявки Администратором ЭДО заявка может быть одобрена или отклонена.
5. Оператор ЭТП обеспечивает заявителю возможность подачи заявки на подключение к функциональности простой электронной подписи.

5.2. Правила создания и выдачи ключей

1. Создание (замена) ключа осуществляется с использованием сервиса генерации ключа на ЭТП. Заявитель вправе самостоятельно произвести замену своего ключа с использованием сервиса генерации ключа.
2. Создаваемый ПИН-код ключа должен содержать только цифровые символы (не менее 8).
3. Оператор ЭТП обязан обеспечить уникальность и конфиденциальность выдаваемых ключей.
4. При использовании простой электронной подписи заявитель в обязательном порядке знакомится с правилами использования простой электронной подписи, опубликованными в открытом доступе на сайте Оператора ЭТП.
5. Владелец ключа простой электронной подписи обязан:
 - обеспечивать конфиденциальность ключа простой электронной подписи;
 - формировать простую электронную подпись на ЭТП с использованием ключа, полученным в порядке, установленном настоящими Правилами;
 - в случае нарушения конфиденциальности ключа или его утери незамедлительно уведомить об этом Администратора ЭДО.

Гражданскую-правовую ответственность за негативные последствия, наступившие в результате несоблюдения владельцем ключа простой электронной подписи перечисленных выше обязанностей, несет владелец ключа простой электронной подписи.

6. Выдача ключа простой электронной подписи заявителю осуществляется Администратором ЭДО на основании полученного заявления на подключение к функциональности простой электронной подписи и результата рассмотрения представленных заявителем запрашиваемых документов и действий:
 - основного документа, удостоверяющего личность заявителя;
 - фото заявителя с основным документом, удостоверяющим личность заявителя (разворот с фотографией);

- для уполномоченного лица - документа, подтверждающего его полномочия действовать от имени другого лица;
- оплаты счета, выставленного Оператором ЭТП за подключение к функциональности простой электронной подписи.

7. Оплата счета, выставленного Оператором ЭТП за подключение юридического лица к функциональности простой электронной подписи должна быть осуществлена исключительно с расчетного счета, открытого на имя указанного юридического лица.

Подтверждением права физического лица действовать от имени юридического лица для целей подключения к функциональности простой электронной подписи являются конклюдентные действия в виде оплаты счета, выставленного Оператором ЭТП за подключение юридического лица к функциональности простой электронной подписи, с расчетного счета данного юридического лица.

8. Оплата счета, выставленного Оператором ЭТП за подключение Участника ЭТП - индивидуального предпринимателя к функциональности простой электронной подписи должна быть осуществлена с расчетного счета, открытого на имя указанного индивидуального предпринимателя.

9. Оплата счета, выставленного Оператором ЭТП за подключение Участника ЭТП - физического лица к функциональности простой электронной подписи должна быть осуществлена банковским переводом с лицевого счета, открытого на имя указанного физического лица или банковским платежом с указанием Ф.И.О. плательщика – указанного физического лица.

10. В случае отклонения Администратором ЭДО заявки на подключение к функциональности простой электронной подписи средства, поступившие в качестве оплаты счета за подключение к функциональности простой электронной подписи возвращаются заявителю – участнику ЭТП.

11. При наличии действующего квалифицированного сертификат ключа проверки электронной подписи, выданного на имя заявителя, подключение к функциональности простой электронной подписи осуществляется на основании данного сертификата. Владельцем простой электронной подписи в этом случае признается владелец действующего квалифицированного сертификата ключа проверки электронной подписи.

12. Для реализации функции обеспечения неизменности электронных документов, подписанных простой электронной подписью, выданной в соответствии с настоящими Правилами, и обнаружения фактов внесения изменений в электронный документ после его подписания, каждый электронный документ, подписанный простой электронной подписью, заверяется подписанием усиленной квалифицированной электронной подписью Оператора ЭТП.

13. Проверка подлинности простой электронной подписи, которой подписан электронный документ, в Системе B2B-Center осуществляется пользователем ЭТП с использованием соответствующего сервиса. Выводится Ф.И.О. и название организации (если подпись выдана уполномоченному лицу организации) – владельца простой электронной подписи, дата и время подписания электронного документа.

6. Использование усиленной электронной подписи

6.1. Удостоверяющие центры и сертификаты ключей проверки ЭП

1. Договор Администратора ЭДО с удостоверяющим центром не является публичной офертой.

Администратор ЭДО вправе отказать в заключении договора удостоверяющему центру без указания причин отказа. Приобретение статуса подключенного удостоверяющего центра включает в себя подключение к Системе ЭДО B2B-Center.

2. Подключение удостоверяющего центра к Системе ЭДО B2B-Center состоит в регистрации в Системе ЭДО подключаемого удостоверяющего центра, действующих корневых и промежуточных сертификатов удостоверяющего центра. Подключенному удостоверяющему центру в Системе ЭДО B2B-Center присваивается статус «подключен».

3. Подключенный удостоверяющий центр может быть отключен от Системы ЭДО с выводом статуса «отключен» и даты отключения.

4. Сертификаты ключей проверки подписей, изготовленные удостоверяющим центром, статус подключенного удостоверяющего центра которого прекращен, начиная с даты расторжения договора с Администратором ЭДО, не могут быть использованы на ЭТП.

5. Администратор ЭДО обеспечивает работу Участников ЭТП с действительными сертификатами ключей проверки подписей, удовлетворяющими требованиям к сертификатам ключей проверки подписей, используемым в Системе ЭДО B2B-Center и выданными подключенными удостоверяющими центрами, выполняющими требования Регламента. Состав и свойства сертификата определяют разделы ЭТП, в работе которых сертификат может применяться.

6. Администратор ЭДО осуществляет регистрацию в Системе ЭДО B2B-Center сертификатов ключей проверки подписей Участников ЭТП. Необходимыми условиями для регистрации сертификата ключа проверки подписи являются следующие:

- на момент регистрации сертификат ключа проверки подписи не внесен в списки отзываемых сертификатов, зарегистрированных в Системе ЭДО;
- корневой/промежуточный сертификат подключенного удостоверяющего центра, выдавшего данный сертификат ключа проверки подписи, зарегистрирован в Системе ЭДО;
- сертификат ключа проверки подписи выдан до даты прекращения статуса партнерского удостоверяющего центра либо организации, представляющей интересы подключенного удостоверяющего центра. Удостоверяющий центр, выдавший сертификат ключа проверки подписи, на момент выдачи сертификата должен иметь в Системе ЭДО статус «подключен».

7. Сертификат ключа проверки подписи признается изданным удостоверяющим центром, если подтверждена подлинность электронной подписи уполномоченного лица удостоверяющего центра с использованием средств электронной подписи и сертификата ключа проверки подписи уполномоченного лица удостоверяющего центра.

8. Идентификационные данные, занесенные в поле «Субъект» (Subject Name) сертификата ключа проверки подписи однозначно идентифицируют владельца сертификата ключа проверки подписи и соответствуют идентификационным данным владельца сертификата ключа проверки подписи, зарегистрированным в реестре сертификатов удостоверяющего центра.

9. Для определения статуса сертификата ключа проверки подписи используется список отзываемых сертификатов. Структура и формат списка отзываемых сертификатов определяются Удостоверяющим центром.

10. Местом публикации списков отзываемых сертификатов принимается адрес информационного ресурса, определенный в расширении CRL Distribution Point сертификата ключа проверки подписи. Сроки изготовления и публикации списка отзываемых сертификатов в точках распространения списков отзываемых сертификатов, порядок и сроки предоставления корневых сертификатов Администратору ЭДО определяются договором Администратора ЭДО с партнерским удостоверяющим центром либо с организацией, представляющей интересы подключенного удостоверяющего центра.

6.2. Средства электронной подписи

1. В качестве средств электронной подписи, обеспечивающих реализацию функций создания и проверки электронной подписи, в Системе ЭДО используются криптографические средства, сертифицированные ФСБ России в системе сертификации РОСС RU.0001.030001, имеющие действующий сертификат соответствия и которые:

- обеспечивают реализацию функций создания электронной подписи в электронном документе с использованием ключа электронной подписи, подтверждения подлинности электронной подписи в электронном документе с использованием ключа проверки подписи, создания ключей и ключей проверки электронных подписей;
- используются совместно со средствами вычислительной техники, общесистемным программным обеспечением и его компонентами, а также иным программно-аппаратным и информационным обеспечением, необходимым для осуществления электронного документооборота в Системе ЭДО.

2. На рабочих местах пользователей электронной подписи допускается применение средств электронной подписи, полученных легальным путем.

3. Применение средства электронной подписи должно осуществляться в соответствии с требованиями формуляра и эксплуатационной документации на данное средство.

4. Владельцы сертификатов ключей проверки подписей самостоятельно обеспечивают сохранность в тайне ключей электронной подписи и несут за это ответственность в соответствии с действующим законодательством Российской Федерации.

6.3. Формирование и проверка усиленной электронной подписи

1. Формирование электронной подписи электронного документа осуществляется с использованием применяемого средства электронной подписи и программного обеспечения ЭТП. Формирование электронной подписи может быть осуществлено только владельцем сертификата ключа проверки подписи, соответствующий ключ электронной подписи которого действует на момент формирования электронной подписи.

2. При создании электронной подписи средства электронной подписи в Системе ЭДО B2B-Center:

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

3. Подтверждение подлинности электронной подписи электронного документа осуществляется с использованием применяемого средства электронной подписи и программного обеспечения ЭТП.

4. Подтверждение подлинности электронной подписи может быть осуществлено владельцами

сертификатов ключей проверки подписей. Владелец сертификата ключа проверки подписи с использованием применяемых средств подтверждения подлинности должен удостовериться, что электронная подпись в электронном документе равнозначна собственноручной, и только после признания электронной подписи равнозначной собственноручной обеспечить исполнение данного электронного документа.

5. При проверке электронной подписи средства электронной подписи в Системе ЭДО B2B-Center:

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

6. Применяемые в Системе ЭДО B2B-Center средства защиты информации достаточны для защиты информации от несанкционированного доступа, для подтверждения авторства, подлинности и целостности электронных документов, а также для разрешения конфликтных ситуаций по ним.

7. При этом субъект Регламента признает, что процедура разрешения конфликтных ситуаций не ущемляет его интересов в сравнении с другими участниками Системы ЭДО.

6.4. Применение усиленной электронной подписи

1. Сертификат ключа проверки усиленной электронной подписи действителен в определенный момент времени при одновременном соблюдении следующих условий:

- сертификат ключа проверки подписи изготовлен подключенным удостоверяющим центром;
- наступил момент начала действия сертификата ключа проверки подписи;
- срок действия сертификата ключа проверки подписи не истек;
- сертификат ключа проверки подписи не аннулирован, и не отозван, а его действие его не приостановлено;
- деятельность удостоверяющего центра не прекращена без передачи его функций другим лицам;
- подтверждена подлинность ключа усиленной электронной подписи удостоверяющего центра в данном сертификате.

Для осуществления проверки подлинности ключа электронной подписи удостоверяющего центра на рабочем компьютере участника ЭТП в соответствующие хранилища сертификатов операционной системы участника ЭТП должны быть установлены корневой и промежуточные сертификаты Удостоверяющего центра.

2. Ключ электронной подписи действителен в определенный момент времени при одновременном соблюдении следующих условий:

- наступил момент начала действия ключа электронной подписи;
- срок действия ключа электронной подписи не истек;
- сертификат ключа проверки подписи, соответствующий данному ключу электронной подписи, действителен.

3. Усиленная электронная подпись в электронном документе действительна при одновременном соблюдении следующих условий:

- на момент подписания электронного документа сертификат ключа проверки подписи, используемый при формировании усиленной электронной подписи, действителен;
- на момент подписания электронного документа ключ усиленной электронной подписи, соответствующий указанному сертификату ключа проверки подписи, действителен;
- подтверждена подлинность усиленной электронной подписи электронного документа на сертификате, относящемся к данной усиленной электронной подписи;
- формирование электронной подписи выполнено без нарушения условий настоящего Регламента;
- усиленная электронная подпись электронного документа сформирована и используется с учетом ограничений, содержащихся в сертификатах лиц, подписывающих электронный документ.

Сертификат ключа проверки подписи в расширении Extended Key Usage содержит области использования сертификата и ключа, устанавливающие право владельца данного сертификата ключа проверки подписи подписывать соответствующие электронные документы.

Требования к перечню областей использования сертификатов ключей проверки подписей, используемых в Системе ЭДО, приведен в Приложении № 1.

4. В Системе ЭДО B2B-Center при использовании усиленных электронных подписей Участники ЭТП обязаны:

- 1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;
- 2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников ЭТП о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- 3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- 4) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ;
- 5) удостовериться в работоспособности ЭП и соответствии всем перечисленным в данном разделе требованиям не более чем за два часа до предполагаемого использования ЭП, а в случае возникновения затруднений в использовании ЭП Участник ЭТП обязан не менее чем за час до предполагаемого использования ЭП обратиться в службу поддержки ЭТП.

5. В Системе ЭДО B2B-Center сертификаты ключей подписей, выданные в соответствии с Федеральным законом от 10 января 2002 года N 1-ФЗ «Об электронной цифровой подписи», признаются квалифицированными сертификатами.

6. В Системе ЭДО B2B-Center электронный документ, подписанный электронной подписью, ключ проверки которой содержится в сертификате ключа проверки электронной подписи, выданном в соответствии с порядком, ранее установленным Федеральным законом от 10 января 2002 года № 1-ФЗ "Об электронной цифровой подписи", в течение срока действия указанного сертификата , но не позднее 31 декабря 2013 года признается электронным документом, подписанным квалифицированной электронной подписью в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ.

7. В Системе ЭДО B2B-Center электронный документ, подписанный электронной подписью, ключ

проверки которой содержится в сертификате ключа проверки электронной подписи, выданном в соответствии с порядком, ранее установленным Федеральным законом от 10 января 2002 года № 1-ФЗ "Об электронной цифровой подписи", в течение срока действия указанного сертификата, с 1 января 2014 года признается электронным документом, подписанным неквалифицированной электронной подписью в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ.

8. В Системе ЭДО B2B-Center электронный документ, подписанный электронной подписью с применением квалифицированного сертификата после 1 июля 2013 г. признается электронным документом, подписанным квалифицированной электронной подписью в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ.

7. Условия признания электронных документов, подписанных электронной подписью, равнозначными документами на бумажном носителе, подписанным собственноручной подписью

1. В Системе B2B-Center информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписенному собственноручной подписью и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации.
2. В Системе B2B-Center информация в электронной форме, подписанная простой электронной подписью и неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписенному собственноручной подписью. Порядок проверки простой электронной подписи и неквалифицированной электронной подписи описан в разделах 5.2 и 6.3.
3. В Системе B2B-Center информация в электронной форме, подписанная простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписенному собственноручной подписью при выполнении условий раздела 5. Использование простой электронной подписи.

8. Порядок разрешения конфликтных ситуаций

8.1. Общие Положения

1. Разрешение конфликтных ситуаций на ЭТП, связанных с применением электронной подписи, осуществляется Согласительной комиссией. Согласительная комиссия создается с целью разрешения конфликтных ситуаций, возникающих в связи с подтверждением подлинности электронной подписи и установления равнозначности электронной подписи собственноручной.
2. При возникновении разногласий Участник ЭТП, заявляющий о разногласии (инициатор), обязан направить Администратору ЭДО (копия – Оператору ЭТП) заявление о разногласиях, подписанное уполномоченным должностным лицом, с подробным изложением причин разногласий и предложением создать комиссию по ее разрешению. Заявление должно содержать фамилии представителей стороны - инициатора, которые будут участвовать в работе комиссии.
3. До подачи заявления стороне - инициатору рекомендуется убедиться в целостности установленного на его технических средствах программного обеспечения, в том числе средства электронной подписи, а также в отсутствии несанкционированных действий со стороны своего персонала и третьих лиц.
4. По заявлению о разногласиях Администратор ЭДО формирует согласительную комиссию, в которую входят:
 - представитель Администратора ЭДО – председатель комиссии;
 - представитель инициатора – член комиссии;
 - представитель ответчика – член комиссии.
5. Члены комиссии от каждой стороны назначаются приказами соответствующей стороны.
6. В качестве эксперта по применению электронной подписи и проведению процедуры подтверждения подлинности электронной подписи привлекается представитель Удостоверяющего центра, выпустившего сертификат ключа проверки подписи инициатора.
7. Комиссия осуществляет свою деятельность по месторасположению Администратора ЭДО.

8.2. Документы, предоставляемые инициатором

1. Сторона-инициатор представляет заявление о разногласии с указанием:

- даты и номера заявления;
- реквизитов инициатора и ответчика;
- обстоятельств, на которых основаны заявленные требования, и сведений о подтверждающих их доказательствах;
- обоснованного расчета заявленных требований;
- нормы законодательных и иных нормативных правовых актов, на основании которых выставляется требование;
- перечня прилагаемых к заявлению о разногласии документов, составляющих доказательную базу. В состав указанных документов должны быть включены:
 - файл, содержащий электронный документ с электронной подписью, либо файл, содержащий электронный документ и файл, содержащий электронную подпись этого документа;
 - файл, содержащий сертификат ключа проверки подписи, соответствующий электронной подписи.

8.3. Порядок работы согласительной комиссии

1. Ответчик обязан в период работы комиссии представить инициатору и комиссии ответы по каждому требованию, изложенному в заявлении о разногласиях.
2. В ответах ответчика на каждое требование должны содержаться документально обоснованные ответы или сделана ссылка на доказательства, которые могут быть представлены в ходе работы комиссии. Любая сторона в ходе работы комиссии может внести ходатайства об изменении или дополнении своих требований или ответов.
3. Комиссия в ходе разбирательства в любой момент может затребовать от сторон предоставления документов, вещественных или иных доказательств в устанавливаемый комиссией срок.
4. Рассмотрение спора производится на основании всех представленных документов и доказательств. В том случае, если обстоятельства, имеющие значение для принятия решения по делу, могут быть исследованы только на основе применения специальных научных знаний, комиссия вправе назначить экспертизу по подтверждению подлинности электронной подписи в электронном документе.
5. Проведение экспертизы возлагается на экспертов Удостоверяющего центра. Запрос на проведение экспертизы оформляется Заявлением на подтверждение подлинности электронной подписи в электронном документе, подающемся в Удостоверяющий центр.
6. Экспертиза может быть назначена комиссией по обоснованному ходатайству любой из сторон или по ее собственной инициативе.
7. Экспертиза осуществляется с использованием применяемого средства электронной подписи и специализированного программного обеспечения (СПО) «Программно-аппаратный комплекс Удостоверяющего центра. Программный комплекс разбора конфликтных ситуаций».
8. Технический порядок проведения экспертизы определяется эксплуатационной документацией на данное СПО.
9. Экспертиза осуществляется на компьютере, конфигурация и технические характеристики которого полностью соответствуют требованиям, изложенным в эксплуатационной документации данного СПО.

8.4. Оформление результатов работы согласительной комиссии

1. По итогам работы согласительной комиссии составляется акт, в котором содержится краткое изложение выводов комиссии и решение комиссии по рассматриваемому разногласию.
2. Помимо изложения выводов согласительной комиссии и решения комиссии акт должен содержать следующие данные:
 - состав комиссии;
 - дату и место составления акта;
 - дату и время начала и окончания работы комиссии;
 - краткий перечень мероприятий, проведенных комиссией;
 - собственоручные подписи членов комиссии;
 - указание на особое мнение члена (или членов комиссии), в случае наличия такового.
3. Акт составляется в 4-х экземплярах и предоставляется Администратору ЭДО, Оператору ЭТП и Участникам ЭТП, полномочные представители которых являлись членами согласительной комиссии.

9. Разграничение ответственности

1. Администратор ЭДО несет ответственность за надлежащее хранение и своевременное уничтожение электронных документов в соответствии с действующим законодательством РФ.
2. Администратор ЭДО не несет ответственность за какой-либо ущерб, потери и прочие убытки, которые понес Участник ЭТП случае:
 - 1) несоответствия указанных в п. 1.5 Регламента программно-технических средств Участника ЭТП, необходимым для работы в Системе ЭДО.
 - 2) ненадлежащего исполнения Участником ЭТП Регламента, несоблюдения руководств, правил, памяток, инструкций, информационных сообщений и новостей, опубликованных на сайте ЭТП и касающихся работы Участника в Системе ЭДО и использования и применения электронной подписи.
 - 3) если информация, размещенная Участником ЭТП в Системе ЭДО, по вине самого Участника ЭТП (пользователя ЭТП) станет известна третьим лицам, которые использовали ее с целью нанести ущерб Участнику ЭТП.

10. Прочие условия

1. Регламент действует и является обязательным для исполнения субъектами Регламента на весь период времени, в течение которого субъект Регламента имеет в своем составе зарегистрированных в Системе ЭДО пользователей.
2. Не менее чем за 5 календарных дней до начала действия новой версии Регламента Администратор ЭДО уведомляет об этом субъектов Регламента посредством публикации новости или направлением информационных сообщений по адресам электронной почты пользователей Системы.
3. Субъект Регламента считается признавшим юридическую обязательность новой версии Регламента, если Администратор ЭДО до даты вступления в силу Регламента не получил от субъекта Регламента сообщения об обратном. Если такое сообщение поступило в устной форме, Субъект Регламента в течение 24 часов после направления устного сообщения должен продублировать это сообщение в письменной форме (по почте или курьером). В день получения Администратором ЭДО сообщения Субъекта Регламента об отказе принять новую версию Регламента, Субъект Регламента отключается от Системы ЭДО. К тем сделкам и действиям (операциям), выполнение которых не завершено на момент отключения Субъекта Регламента от Системы ЭДО, и которые должны быть закончены после вступления в силу новой версии Регламента, применяется версия Регламента, действовавшая на момент заключения таких сделок и/или начала выполнения соответствующих действий (операций).

Приложения

Приложение №1

к Регламенту организации
электронного документооборота
и использования электронной подписи

Требования к сертификатам ключей проверки подписей, используемым в Системе ЭДО B2B-Center

1. Форма (состав полей) квалифицированного сертификата ключа проверки электронной подписи, используемого в Системе ЭДО B2B-Center должна соответствовать требованиям, указанным в Приказе от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
2. В квалифицированном сертификате ключа проверки подписи должна содержаться следующая информация:
 - 1) уникальный номер квалифицированного сертификата, даты начала и окончания его действия;
 - 2) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата - для физического лица либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата - для юридического лица;
 - 3) страховой номер индивидуального лицевого счета владельца квалифицированного сертификата - для физического лица либо идентификационный номер налогоплательщика владельца квалифицированного сертификата - для юридического лица;
 - 4) ключ проверки электронной подписи;
 - 5) наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Федеральным законом;
 - 6) наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат, номер квалифицированного сертификата удостоверяющего центра;
 - 7) ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются);
 - 8) иная информация о владельце квалифицированного сертификата (по требованию заявителя).
3. Сертификат ключа проверки подписи для бесплатной регистрации должен содержать в расширении «Улучшенный ключ» сертификата OID 1.2.643.6.7 (Использование в работе систем электронного документооборота и электронных торговых систем B2B-CENTER), устанавливающий правомерность использования сертификата ключа проверки подписи на ЭТП (в Системе электронных торгов B2B-Center). Требования настоящего пункта не распространяются на случаи участия в закупке в порядке ст. 3.4 Федерального закона №223-ФЗ "О закупках".
4. Сертификаты ключа проверки подписи, не отвечающие требованиям, указанным в предыдущем

пункте, регистрируются в соответствии с тарифами, опубликованными на сайте Системы электронных торгов B2B-Center.