

«УТВЕРЖДАЮ»

Генеральный директор



Карпов А.Г.

«07» Января 2010 г.

РЕГЛАМЕНТ

применения средств криптографической защиты информации при
защищенном обмене электронными документами

Версия 5.0

Оглавление

| | |
|--|----|
| ВВЕДЕНИЕ | 3 |
| ТЕРМИНЫ И СОКРАЩЕНИЯ | 4 |
| ОБЩИЕ ПОЛОЖЕНИЯ..... | 7 |
| ОБЩИЕ ВОПРОСЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ | 8 |
| ПОРЯДОК РЕГИСТРАЦИИ В СИСТЕМЕ. ПОРЯДОК ПОЛУЧЕНИЯ СКЗИ, КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТОВ..... | 8 |
| ФУНКЦИИ И ЗАДАЧИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА | 10 |
| ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ И ВЛАДЕЛЬЦА СКП..... | 12 |
| ДЕЙСТВИЯ СТОРОН ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ | 14 |
| ДЕЙСТВИЯ СТОРОН ПРИ ИЗМЕНЕНИИ ДАННЫХ ВЛАДЕЛЬЦА, УКАЗАННЫХ В СЕРТИФИКАТЕ КЛЮЧА ПОДПИСИ..... | 15 |
| ДЕЙСТВИЯ СТОРОН ПРИ НЕСОБЛЮДЕНИИ ПРАВИЛ ЭКСПЛУАТАЦИИ КЛЮЧЕВОГО НОСИТЕЛЯ ВЛАДЕЛЬЦЕМ | 15 |
| КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ..... | 16 |
| ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ СИСТЕМЫ | 16 |
| ПОРЯДОК ВЗАИМОДЕЙСТВИЯ СТОРОН ПРИ НЕШТАТНЫХ СИТУАЦИЯХ, СВЯЗАННЫХ С ЭКСПЛУАТАЦИЕЙ СКЗИ | 17 |
| ПРОЧИЕ УСЛОВИЯ..... | 17 |
| ПРИЛОЖЕНИЯ | 17 |

ВВЕДЕНИЕ

- 1.1. Настоящий Регламент разработан на основании действующего законодательства Российской Федерации, а также учредительных и иных документов Удостоверяющего центра, Организатора Системы и определяет:
 - Порядок организации криптографической защиты информации при обмене электронными документами.
 - Порядок регистрации и подключения Пользователей и Владельцев сертификатов ключей подписей (далее – СКП) к автоматизированной информационной системе подготовки, формирования и передачи электронных документов в виде юридически значимых электронных документов по открытым каналам связи (далее – Система).
- 1.2. Организатором Системы является ООО "РТС - Тендер".
- 1.3. Деятельность по обслуживанию средств, предназначенных для криптографической защиты конфиденциальной информации, а также выполнение функций Удостоверяющего Центра в рамках Системы выполняется ЗАО «АНК» (далее – Удостоверяющий Центр).
- 1.4. Владельцы сертификатов ключей подписей используют для защиты информации сертифицированные, в порядке, установленном законодательством Российской Федерации, средства электронной цифровой подписи (далее – ЭЦП), позволяющие идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации, в электронном виде.
- 1.5. Владельцы сертификатов ключей подписей используют для защиты информации, при передаче её по открытым каналам связи, сертифицированные, в порядке, установленном законодательством Российской Федерации, средства криптографической защиты информации (далее – СКЗИ).
- 1.6. Используемые заверенные ЭЦП электронные документы во взаимоотношениях между Пользователями и Владельцами сертификатов ключей подписей, являются оригиналами, имеют юридическую силу, подлежат хранению в хранилище юридически значимых документов и могут использоваться в качестве доказательств в суде, а также при рассмотрении споров в досудебном порядке.

Примечание: Если Пользователь или Владелец сертификата ключа подписи, являющиеся должностными лицами какой-либо организации, с целью контроля самостоятельно или по согласованию с Организатором системы переносит информацию, представленную в электронном виде по каналам связи, на бумажный носитель, то на первом листе бумажной копии следует отметить, что оригинал был отправлен в электронном виде, и указать данные электронного документа (электронная цифровая подпись, наименование юридического лица или фамилия, имя, отчество физического лица - отправителя электронного документа, электронный адрес отправителя электронного документа) - оригинала, заверив подписью Владельца сертификата ключа подписи и печатью организации, сотрудником которой является Владелец сертификата ключа подписи.
- 1.7. Пользователи признают, что использование в Системе сертифицированных СКЗИ, которые реализуют ЭЦП и шифрование, достаточно для обеспечения конфиденциальности информационного взаимодействия пользователей, а также подтверждения того, что электронный документ:
 - исходит от Владельца сертификата ключа подписи (подтверждение авторства документа);
 - не претерпел изменений при информационном взаимодействии Пользователя (подтверждение целостности и подлинности документа).

- 1.8. Регламент начинает действовать в отношении Заявителя на сертификат ключа подписи с момента заключения им (Участником информационной системы) Договора с Удостоверяющим Центром или с Центром регистрации. При обмене электронными документами в Информационной Системе Пользователи и Владельцы сертификатов ключей подписей должны руководствоваться положениями настоящего Регламента.

ТЕРМИНЫ И СОКРАЩЕНИЯ

Администратор УЦ – должностное лицо Удостоверяющего Центра, обрабатывающее заявление на издание сертификата ключа подписи.

Абонент – субъект, которому издан сертификат ключа подписи.

Аутентификация информации - подтверждение подлинности и целостности информации, содержащейся в документе. Аутентификация может осуществляться как на основе структуры и содержания документа или его реквизитов, так и путем реализации криптографических алгоритмов преобразования информации. Доказательная аутентификация информации осуществляется анализом (экспертизой) подписей должностных лиц и печатей на бумажных документах или проверкой правильности ЭЦП.

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

Доверенное лицо – физическое лицо, которому Заявитель на сертификат ключа подписи доверяет присутствовать вместо себя на этапе генерации ключей подписи, получить ключевой носитель с сертификатом в Удостоверяющем Центре, совершать иные действия от лица и в интересах Заявителя.

Договор – Договор, заключенный между участником информационной системы и Удостоверяющим Центром. Договор определяет состав, порядок исполнения и стоимость услуг, оказываемых Владельцу СКП Удостоверяющим Центром.

Закрытый (секретный) 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. Закрытые ключи хранятся Владельцами в тайне. Закрытые ключи используются для формирования ЭЦП Владельца и дешифрования.

Замена сертификата ключа подписи – издание сертификата взамен выведенного из обращения по гарантии на оставшееся время действия договора.

Заявитель – физическое лицо, уполномоченное участником информационной системы для ведения защищенного документооборота, подающее свои персональные данные и непосредственно участвующие в процессе заключения Договора для получения сертификата ключа подписи в Удостоверяющем Центре.

Система – корпоративная информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением ее участников, представляющая собой совокупность вычислительных средств, программного обеспечения, телекоммуникационных средств, другого оборудования, и предназначенная

для формирования, приема-передачи электронных документов, заверенных электронно-цифровой подписью.

Издание сертификата ключа подписи – комплекс работ и услуг по созданию ключей электронной цифровой подписи, изготовлению и выдаче сертификата ключа подписи в форме электронного документа, с последующим внесением в реестр изданных сертификатов и публикация на портале.

В соответствии с изданным СКП для него оформляется 2 (Два) сертификата на бумажном носителе.

Ключевой носитель – отчуждаемый защищенный носитель (eToken, Rutoken, SmartCard и т.п.), содержащий один или несколько ключей.

Компрометация ключа - утрата доверия к тому, что используемые закрытые ключи недоступны посторонним лицам. К событиям, связанным с компрометацией ключей, относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение в Системе;
- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания;
- утрата ключей от сейфов (помещений) в момент нахождения в них ключевых носителей;
- утрата ключей от сейфов (помещений) в момент нахождения в них ключевых носителей с последующим обнаружением;
- доступ посторонних лиц к ключевой информации;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе, когда ключевой носитель вышел из строя и не опровергнута возможность того что, данный факт произошел в результате несанкционированных действий злоумышленника);
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к закрытым ключам электронной цифровой подписи.

Конфиденциальная информация - информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, а также настоящим Регламентом и требующая защиты.

Конфликтная ситуация - ситуация, при которой у пользователей Системы возникает необходимость разрешить вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных средствами криптографической защиты информации.

Ключ (криптографический ключ) – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразования.

Некорректный электронный документ - электронный документ, не прошедший процедуры проверки ЭЦП, имеющий искажения в тексте сообщения, не позволяющие понять его смысл.

Несанкционированный доступ (НСД) к информации - доступ к информации, нарушающий установленные правила ее получения.

Организатор Системы – ООО "РТС - Тендер"

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе. Открытый ключ Владельца сертификата ключа подписи является действующим на момент подписания, если он зарегистрирован (сертифицирован) и введен в действие.

Открытый ключ шифрования – криптографический ключ, предназначенный для шифрования разового (сеансового) ключа шифрования с целью его передачи адресату по открытым каналам связи. Открытые ключи шифрования могут быть известны всем пользователям системы.

Парольная фраза – словосочетание, позволяющее аутентифицировать владельца СКП для управления сертификатом по неавторизованным каналам связи. Меняется ежегодно вместе с сертификатом ключа подписи для каждого владельца СКП.

Переиздание сертификата ключа подписи – деятельность УЦ по продлению действия СКП на новый период.

Пользователь – физическое лицо, использующее полученные в Удостоверяющем Центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи Владельцу сертификата ключа подписи или использующее этот сертификат.

Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе Владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Сертификат ключа подписи (СКП) - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего Центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются Удостоверяющим Центром Участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

СОС (Список отозванных сертификатов, Certificate Revocation List, CRL) – список отозванных сертификатов.

Средства криптографической защиты информации (СКЗИ) – средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

Средство Вычислительной Техники (далее СВТ) — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций – создание электронной цифровой подписи 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.

Удостоверяющий центр¹ – информационная система ЗАО «АНК», обеспечивающая сертификацию открытых ключей пользователей Системы и выполняющая иные, предусмотренные Федеральным законом от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» функции.

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей подписей и списков отозванных сертификатов.

Управление ключами - создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение, а также издание, приостановление и аннулирование сертификатов открытых ключей в соответствии с политикой безопасности Удостоверяющего Центра.

Участник системы – юридическое или физическое лицо, участник обмена электронными документами в Системе, заключивший с Удостоверяющим центром договор, и признающий данный Регламент.

Целостность информации – способность автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

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

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать Владельца сертификат ключа подписи, а также установить отсутствие искажения информации в электронном документе. В соответствии с ФЗ «Об Электронной цифровой подписи» признается аналогом собственноручной подписи.

ОБЩИЕ ПОЛОЖЕНИЯ

- 3.1. Пользователи Системы осуществляют обмен электронными документами по открытым каналам связи и соблюдают требования регламента.
- 3.2. Пользователи системы соблюдают установленную в соответствии с требованиями документа «КриптоПро CSP. Инструкция по использования» (поставляется в электронном виде) последовательность действий по установке, настройке и работе СКЗИ «КриптоПро CSP».
- 3.3. Удостоверяющий Центр осуществляет работы по управлению ключами в соответствии с требованиями Федерального Закона «Об электронной цифровой подписи», положениями настоящего Регламента, на основании Договора между Удостоверяющим Центром и Участником информационной системы.
- 3.4. В случае нарушения правил использования СКЗИ и/или возникновения конфликтных ситуаций, связанных с подтверждением авторства и/или подлинности электронных документов, заверенных ЭЦП, или иных конфликтных ситуаций,

¹ Когда речь идет об информационной системе, второе слово в словосочетании Удостоверяющий центр пишется с маленькой буквы. В случае если упоминается организация, исполняющая роль Удостоверяющего Центра системы – оба слова пишутся с большой буквы.

связанных с использованием ЭЦП, Стороны руководствуются Порядком разрешения конфликтных ситуаций, изложенным в Приложении №1 к настоящему Регламенту.

ОБЩИЕ ВОПРОСЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

- 4.1. Заявитель, при необходимости, предоставляет Удостоверяющему Центру право создать закрытый и открытый ключи ЭЦП и шифрования на Автоматизированном рабочем месте оператора удостоверяющего центра (АРМ УЦ). При этом в целях обеспечения безопасности ключей, по умолчанию они создаются без возможности копирования их с ключевого носителя.
 - 4.2. Удостоверяющий Центр издает сертификаты ключей подписей в электронном виде и в виде документа на бумажном носителе. При издании сертификатов ключей подписи Удостоверяющий Центр оформляет два экземпляра сертификата в форме документов на бумажном носителе, которые заверяются собственноручными подписями Владельца сертификата ключа подписи и уполномоченного лица Удостоверяющего Центра, а также печатью Удостоверяющего Центра. Один экземпляр сертификата ключа подписи на бумажном носителе выдается Владельцу сертификата ключа подписи, второй – остается в Удостоверяющем Центре.
 - 4.3. Удостоверяющий Центр использует программные и технические средства генерации ключевой информации в неизменном виде по отношению к сертифицированному эталону. Удостоверяющий Центр гарантирует отсутствие привнесенных нерегламентированных процедур скрытого копирования индивидуальной секретной ключевой информации в используемых программных и технических средствах.
 - 4.4. Участники системы получают доступ к реестру сертификатов Удостоверяющего Центра и списку отозванных сертификатов. Реестр сертификатов и СОС публикуется на сайте Удостоверяющего Центра в сети Интернет по адресу: <http://www.ank-pki.ru/certstore/public/store> и на резервном сайте («зеркале») по адресу: <http://www.gaz-is.ru/ank/ankpublicca2010.crl>; <http://www.rnt.ru/ank/ankpublicca2010.crl>
- Примечание:** Удостоверяющий Центр принимает все возможные меры, чтобы в кратчайшие сроки внести в СОС сертификаты недействительных (скомпрометированных) ключей.
- 4.5. Срок действия ключей электронных цифровых подписей Владельцев сертификатов ключей подписи составляет 1 (Один) год. Начало периода действия ключей Владельца сертификата ключа подписи исчисляется с даты и времени начала действия соответствующих им сертификатов ключей подписи.

ПОРЯДОК РЕГИСТРАЦИИ В СИСТЕМЕ. ПОРЯДОК ПОЛУЧЕНИЯ СКЗИ, КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТОВ

- 5.1. Для заключения договора с Удостоверяющим центром Заявитель на сайте Удостоверяющего центра формирует Заявку. Формирование Заявки представляет собой заполнение Пользователем Системы специальной взб-формы Заявки, содержащей сведения о наименовании организации, банковских реквизитах организации, руководителе организации, Владельце СКП.
Сформированная Заявка пользователя Системы поступает Администратору УЦ.
- 5.2. Администратор УЦ, в течение 1 (Одного) рабочего дня с момента получения Заявки:
 - обрабатывает данные, содержащиеся в Заявке (проверка, уточнение);

- осуществляет подготовку Договора между Удостоверяющим центром и пользователем Системы.

В случае необходимости, указанной в Заявке:

- документов о предоставлении прав на использование пользователем Системы средства ЭЦП;
- счетов на оплату
 - поставки пользователю Системы ключевого носителя и средства ЭЦП;
 - услуг по предоставлению руководств по установке и настройке средств ЭЦП и работе в Системе (на CD);
 - услуг Удостоверяющего Центра по изданию и гарантийному обслуживанию СКП.

В случае наличия в заявке погрешностей (ошибок) допущенных Заявителем, срок обработки Заявки и подготовки документов может быть увеличен до момента их полного устранения.

5.3. Администратор УЦ направляет в адрес Заявителя (по электронной почте) комплект подготовленных документов (Договор, лицензионный Договор, счета).

5.4. Заявитель, заключив (подписав) Договор с Удостоверяющим центром и оплатив выставленные счета, формирует:

- Заявление на издание удостоверяющим центром СКП;
- прилагаемые к Заявлению документы (копии документов), согласно «Перечня приложений к заявлению на издание сертификата ключа подписи».

5.5. Заявитель (или доверенное лицо Заявителя) в согласованное с УЦ время либо лично прибывает в ЦР для изготовления СКП, либо формирует запрос на сертификат на технических средствах Заявителя.

5.6. Сертификат издается при личном прибытии в Удостоверяющий центр:

5.6.1. Заявитель (или доверенное лицо Заявителя) в согласованное с УЦ время лично прибывает в УЦ для изготовления СКП.

В случае прибытия в УЦ доверенного лица Заявителя, данное лицо должно иметь оформленную Доверенность на присутствие при издании СКП. Форма Доверенности приведена в Приложении № 1 к настоящему Регламенту.

5.6.2. При личном прибытии Заявителя в Центр Регистрации Администратором УЦ производятся процедуры идентификации личности Заявителя, проверка состава, полноты и действительности представленных Заявителем Документов. В случае несоответствия Удостоверяющий центр имеет право отложить издание сертификата ключа подписи до момента исправления данных. При положительных результатах идентификации и проверки выполняются следующие действия:

- На основании Заявления на издание удостоверяющим центром СКП, Администратор УЦ в присутствии Заявителя выполняет на защищенном ключевом носителе Заявителя, действия по инициализации ключевого носителя, генерации ключей электронной цифровой подписи с размещением их в защищенное хранилище ключевого носителя, формированию Запроса на изготовление СКП.
- Администратор УЦ изготавливает СКП: в форме электронного документа и в форме документа на бумажном носителе. СКП в форме документа на бумажном носителе заверяется подписью уполномоченного лица УЦ и печатью УЦ.

- Администратор УЦ размещает на ключевой носитель корневой сертификат Удостоверяющего центра и передает Заявителю ключевой носитель. Лицо, указанное в Заявлении на издание СКП становится Владельцем СКП.
- 5.6.3. Заявитель получает от Администратора УЦ и подписывает 2 экземпляра СКП на бумажном носителе, финансовые документы. В случае, если в Центре Регистрации при изготовлении СКП присутствовало доверенное лицо, то оно обязано передать СКП в форме документа на бумажном носителе Владельцу СКП. Подписанный Владельцем СКП сертификат в форме документа на бумажном носителе направляется в УЦ.
- 5.6.4. Владелец СКП получает от Оператора ЦР инструктаж по правилам работы с СКЗИ, ключами ЭЦП и сертификатами ключей подписи, по порядку доступа к актуальному Реестру сертификатов и СОС.
- 5.6.5. Оператор ЦР передает Владельцу СКП парольную фразу для связи в случае компрометации закрытых ключей. Владелец СКП обеспечивает конфиденциальность парольной фразы.
- 5.6.6. Заявитель или его доверенное лицо получает² и подписывает акт оказанных услуг, товарную накладную о получении комплекта в составе:
- Лицензия(и) на право использования СКЗИ (при наличии в комплекте поставки);
 - Ключевой(ые) носитель(и) с установленными криптографическими ключами электронных цифровых подписей и сертификатом ключа подписи (при наличии в комплекте поставки);
 - Других товарно-материальных ценностей (USB-удлинитель, карт-ридер и пр.) (при наличии в комплекте поставки);
- Либо передает участнику информационной системы, заключившему договор с Удостоверяющим Центром, для подписи - акт оказанных услуг, товарную накладную и пересылает один подписанный экземпляр данного комплекта документов в Удостоверяющий Центр.

ФУНКЦИИ И ЗАДАЧИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

- 6.1. Удостоверяющий Центр предоставляет услуги в соответствии с положениями Федерального закона от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», а именно:
- создает ключи электронных цифровых подписей по обращению Заявителя с гарантией сохранения в тайне закрытых ключей;
 - изготавливает сертификаты ключей подписей на основании надлежащим образом оформленного Заявления и всех необходимых документов, согласно Приложению № 1 к Договору;
 - обеспечивает уникальность ключей сертификатов электронной подписи;
 - изготавливает сертификаты ключа подписи в форме документа на бумажном носителе и в электронном виде;
 - ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему Пользователей;
 - вносит сертификаты ключей подписи в реестр изданных сертификатов ключей не позднее даты начала их действия (публикует);

² При наличии доверенности на получение ТМЦ и доверенности на подпись акта оказанных услуг либо печати участника информационной системы (организации) либо права подписи финансовых документов.

- предоставляет Пользователям доступ к реестру изготовленных сертификатов ключей подписи и списку отозванных сертификатов;
 - обеспечивает выпуск и обновление списка отозванных и аннулированных сертификатов с указанием даты и времени аннулирования сертификата ключа подписи и причину.
- 6.2. Удостоверяющий Центр уведомляет владельцев СКП о фактах, которые стали ему известны и которые существенным образом могут сказаться на возможности дальнейшего использования СКЗИ и сертификата ключа подписи;
- 6.3. Удостоверяющий Центр обязан аннулировать сертификат ключа подписи:
- По истечении срока его действия;
 - При утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационной системе;
 - В случае если Удостоверяющему Центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;
 - По заявлению в письменной форме Владельца сертификата ключа подписи;
 - При компрометации или подозрении на компрометацию ключа подписи;
 - При не соблюдении требований обязательных для выполнения Абонентом;
 - При изготовлении сертификата ключа подписи с ошибками;
 - При прекращении деятельности УЦ АНК;
 - В иных установленных нормативными правовыми актами или соглашением сторон случаях;
- 6.3.1. Удостоверяющий центр аннулирует сертификат ключа подписи после предоставления Участником информационной системы заявления на аннулирование сертификата ключа подписи с указанием причины аннулирования (Приложение № 3 к Регламенту). Участник информационной системы первоначально может предоставить Заявление:
- по электронной почте подписанным сообщением;
 - телефону с указанием парольной фразы;
 - личным прибытием с удостоверяющими личность документами.
- В первых двух случаях необходимо отправить оригинал подписанного Заявления по почте в адрес Удостоверяющего центра в ближайший рабочий день;
- 6.3.2. Удостоверяющий Центр оповещает пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и ответственное лицо (организацию).
- 6.4. Удостоверяющий Центр обязан приостановить действие сертификата ключа подписи:
- по заявлению владельца сертификата ключа подписи;
 - по указанию полномочного лица (Организатора системы) на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или Договором.

Удостоверяющий центр приостанавливает действие сертификата ключа подписи, по заявлению на приостановление действия сертификата (Приложение № 4 к Регламенту) от Владельца сертификата ключа подписи или от организатора системы с указанием

причины и сроком приостановления в течение 1 рабочего дня с момента получения. Временем получения заявления считается:

- при передаче по электронной почте – время передачи сообщения на почтовый сервер ЗАО «АНК»;
 - при вручении лично или передачей иными способами – время получения.
- 6.4.1. Удостоверяющий центр оповещает об этом пользователей путем внесения в СОС соответствующей информации с указанием даты приостановления действия сертификата ключа подписи, а также извещает об этом Владельца сертификата ключа подписи и полномочное лицо (организацию), от которого получено заявление на приостановление действия сертификата ключа подписи;
- 6.4.2. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (организации). В случае если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.
- 6.5. Удостоверяющий центр обеспечивает хранение сертификатов ключей подписей в форме электронных документов после аннулирования не менее трех лет. По истечении указанного срока хранения, сертификаты ключей подписи исключаются из реестра сертификатов ключей подписей и переводятся в режим архивного хранения. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.
- 6.6. Удостоверяющий Центр участвует в работе Экспертной комиссии при рассмотрении конфликтных ситуаций;
- 6.7. Удостоверяющий Центр контролирует правила использования СКЗИ Владельцами сертификатов ключей подписи.

ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ И ВЛАДЕЛЬЦА СКП

- 7.1. Заявитель обязан предоставить достоверную регистрационную и идентифицирующую его информацию в объеме, определенном положениями настоящего Регламента и Договором;
- 7.2. Владелец сертификата ключа подписи, и (или) лицо, ответственное за СКЗИ и уполномоченное для ведения электронного документооборота, в соответствии с Договором, лицензионным соглашением и эксплуатационной документацией на СКЗИ, подготавливает и содержит в рабочем состоянии персональную электронно-вычислительную машину (ПЭВМ) и программное обеспечение, предназначенные для работы в Информационной системе. Владельцу (Заявителю) рекомендуется не использовать средства разработки и отладки программ на ПЭВМ, на которой установлено СКЗИ;
- 7.3. Владелец обязан соблюдать правила эксплуатации ключевого носителя:
- 7.3.1. Ключевой носитель подключается только через USB-порт компьютера и может выполнять своё функциональное назначение только на вычислительных средствах, на которых установлено необходимое программное обеспечение. Загорание светового индикатора свидетельствует о готовности устройства к работе;
- 7.3.2. При получении ключевого носителя из Удостоверяющего Центра, необходимо сменить PIN-код пользователя и пароль администратора;

- 7.3.3. Пароль администратора необходимо держать в запечатанном конверте в труднодоступном месте;
- 7.3.4. PIN-код пользователя должен быть известен только Владельцу СКП. Пароль администратора может знать:
- Администратор безопасности;
 - Лицо ответственное за электронный документооборот и СКЗИ;
 - Владелец СКП, при отсутствии других административных должностей обслуживания СКЗИ.
- 7.3.5. В процессе эксплуатации ключевого носителя Владелец СКП не может удалять контейнер СКП без согласования с администратором УЦ;
- 7.3.6. При наличии доступной в ПО управления ключевыми носителями (RTE - eToken Properties, pki-CLIENT и др.) функции «Форматирование» или «Инициализация», Владелец СКП не должен использовать эту функцию без согласования с администратором УЦ.
- 7.4. Владелец сертификата ключа подписи обязан организовать режим функционирования рабочих мест таким образом, чтобы исключить возможность доступа к СКЗИ, несанкционированной модификации или использования СКЗИ лицами, не имеющими допуска к работе с СКЗИ, а также исключить возможность использования ключей электронных цифровых подписей не уполномоченными на то лицами;
- 7.5. Владелец сертификата ключа подписи обязан при разрешении конфликтных ситуаций, связанных с установлением подлинности и/или авторства спорного документа или иных конфликтных ситуаций связанных с использованием ЭЦП, предоставлять Экспертной комиссии, создаваемой и действующей в соответствии с Приложением № 1 к настоящему Регламенту, все документы и материалы, относящиеся к предмету конфликтной ситуации;
- 7.6. Переиздание сертификата ключа подписи Владельца сертификата ключа подписи производится по инициативе Участника Системы, но не реже одного раза в год (отдельным решением могут быть установлены другие сроки) в следующем порядке:
- Владелец сертификата ключа подписи направляет в Удостоверяющий Центр Заявление на издание сертификата ключа подписи (рекомендуется за месяц до окончания срока действия истекающего сертификата ключа подписи);
 - Удостоверяющий Центр согласовывает с Владельцем сертификата ключа подписи время оказания услуги;
 - Владелец сертификата ключа подписи оплачивает услуги по изданию нового сертификата ключа подписи (если причина переиздания сертификата не подпадает под условия гарантийного обслуживания СКП);
 - Услуги по изданию нового сертификата ключа подписи оказываются Удостоверяющим Центром в соответствии с 5 разделом настоящего Регламента;
 - Владелец сертификата ключа подписи после получения нового сертификата ключа подписи проверяет его работоспособность;
 - Владелец сертификата ключа подписи и (или) лицо, ответственное за СКЗИ и ответственное за электронный документооборот принимает решение о сроках и порядке архивного хранения или об уничтожении старых ключей и соответствующих сертификатов ключей подписи.

Примечание: В случае уничтожения старых ключей – предварительно необходимо расшифровать все электронные документы, зашифрованные с их использованием. Без соответствующих ключей расшифровать документы будет невозможно!

- Владелец обеспечивает хранение расшифрованных документов в электронном виде в соответствии с требованиями, установленными законодательством.
 - Удостоверяющий Центр аннулирует переизданные (замененные) сертификаты ключей подписи.
- 7.7. Владелец сертификата ключа подписи имеет право:
- Не принимать к исполнению электронные документы, заверенные ЭЦП, если:
 - сертификат ключа подписи отправителя утратил силу (не действует, находится в СОС³) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

Примечание: перед принятием решения по исполнению полученного электронного документа, в зависимости от его важности, Владелец сертификата ключа подписи самостоятельно определяет необходимость проверки нахождения сертификата ключа подписи отправителя в СОС.

- не подтверждена подлинность ЭЦП в электронном документе;
 - ЭЦП используется не в соответствии со сведениями, указанными в сертификате ключа подписи.
- Запрашивать подтверждение по полученным им электронным документам в случае возникновения сомнений;
 - Требовать от Удостоверяющего Центра аннулирования своего сертификата ключа подписи в случае наступления событий, трактуемых как компрометация ключевой информации;
 - Требовать исполнения обязательств от других пользователей Информационной системы по принятым ими электронным документам;
 - В случае возникновения конфликтной ситуации, связанной с установлением подлинности и/или авторства спорного документа, требовать разрешения указанных вопросов Экспертной комиссией в соответствии с согласованным порядком.

ДЕЙСТВИЯ СТОРОН ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

- 8.1. Удостоверяющий Центр в момент генерации и сертификации ключей электронных цифровых подписей передает Владельцу сертификат ключа подписи, парольную фразу для связи в случае компрометации закрытых ключей. Владелец сертификата ключа подписи и (или) лицо, ответственное за СКЗИ и уполномоченное для ведения электронного документооборота, обеспечивает сохранение конфиденциальности парольной фразы и ключей электронной цифровой подписи.
- 8.2. При компрометации ключа, Владелец сертификата ключа подписи должен прекратить обмен электронными документами с другими пользователями, немедленно информировать Удостоверяющий Центр о наступлении события согласно п. 6.3.1;
- 8.3. Удостоверяющий Центр, в течении рабочего дня с момента получения заявления аннулирует скомпрометированные ключи и публикует СОС;

³ Актуальный список отозванных сертификатов опубликован на портале доступа к общедоступным компонентам Удостоверяющего Центра в Интернет по адресу <http://www.ank-pki.ru/certsrv/ankpublicca.crl> и на резервном портале («зеркале») по адресу: <http://rep.top-cross.ru/mirror/ank/ankpublicca.crl>

- 8.4. Владелец сертификата ключа подписи, объявивший о компрометации собственных ключей электронных цифровых подписей, в течение одного рабочего дня направляет копию Заявления на аннулирование сертификата ключа подписи по электронной почте или факсу, и оригинал Заявления по почте (Приложение № 3 к настоящему Регламенту) в Удостоверяющий Центр.
- 8.5. В случае если между Участником информационной системы (организацией, сотрудником которой является Владелец сертификата ключа подписи) и Удостоверяющим Центром заключен Договор, не предусматривающий гарантийного обслуживания, Участник системы, допустивший компрометацию собственных ключей электронных цифровых подписей, несет все издержки, связанные с сертификацией и вводом в действие новых ключей электронных цифровых подписей. Если гарантийное обслуживание предусмотрено Договором, сертификация и ввод в действие новых ключей электронных цифровых подписей после события компрометации осуществляется Удостоверяющим Центром в рамках гарантийного обслуживания.

ДЕЙСТВИЯ СТОРОН ПРИ ИЗМЕНЕНИИ ДАННЫХ ВЛАДЕЛЬЦА, УКАЗАННЫХ В СЕРТИФИКАТЕ КЛЮЧА ПОДПИСИ

- 9.1. При изменении данных Владельца сертификата ключа подписи, указанных в сертификате (в случае увольнения и назначение нового сотрудника⁴, изменение должности, наименования подразделения, адреса электронной почты и т.д.), Участник информационной системы (организация, сотрудником которой является Владелец) направляет в адрес Удостоверяющего Центра Заявление на аннулирование сертификата ключа подписи (№ 3 к настоящему Регламенту) с указанием причины аннулирования сертификата, а так же Заявление на издание сертификата ключа подписи с новыми данными Владельца.
- 9.2. В случае если между Участником системы (организацией, сотрудником которой является Владелец) и Удостоверяющим Центром заключен Договор, предусматривающий гарантийное обслуживание, при изменении данных владельца сертификатов ключа подписи аннулирование старого и издание нового сертификата ключа подписи осуществляется Удостоверяющим Центром в рамках гарантийного обслуживания, иначе Участник системы несет все издержки, связанные с сертификацией и вводом в действие новых ключей ЭЦП самостоятельно.

ДЕЙСТВИЯ СТОРОН ПРИ НЕСОБЛЮДЕНИИ ПРАВИЛ ЭКСПЛУАТАЦИИ КЛЮЧЕВОГО НОСИТЕЛЯ ВЛАДЕЛЬЦЕМ

- 10.1. При несоблюдении правил эксплуатации ключевого носителя, описанных в п. 7.3 настоящего Регламента, приведшим к поломке ключевого носителя и дальнейшем необходимости аннулирования старого и издания нового сертификата ключа подписи, Участник информационной системы направляет в адрес Удостоверяющего Центра Заявление на аннулирование сертификата ключа подписи (№ 3 к настоящему Регламенту) с указанием причины аннулирования сертификата, а так же Заявление на издание сертификата ключа подписи с новыми данными Владельца, подтвержденными документально.

⁴ В этом случае необходимо предоставить приказ о назначении нового сотрудника уполномоченным для ведения электронного документооборота и приказ о назначении на должность.

- 10.2. В случае если между Участником системы и Удостоверяющим Центром заключен Договор, предусматривающий гарантийное обслуживание, при данных обстоятельствах аннулирование старого и издание нового сертификата ключа подписи осуществляется Удостоверяющим Центром в рамках гарантийного обслуживания, иначе Участник системы несет все издержки, связанные с сертификацией и вводом в действие новых ключей ЭЦП самостоятельно.

КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

- 11.1. Удостоверяющий Центр и Участник системы в процессе работы в Системе обязаны обеспечить сохранность конфиденциальной информации, полученной друг от друга в соответствии с действующим законодательством Российской Федерации.
- 11.2. Удостоверяющий Центр обязан не разглашать (публиковать) информацию, полученную от Участника Системы, за исключением регистрационной информации включенной в изготовленные сертификаты ключа подписи.
- 11.3. Порядок предоставления конфиденциальной информации налоговым, правоохранительным и судебным органам осуществляется в соответствии с действующим законодательством Российской Федерации.

ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ СИСТЕМЫ

- 12.1. Участник информационной системы несет ответственность за достоверность сведений указанных в Заявлении (Приложение №1 к Договору), а также обязан сообщать обо всех изменениях этих сведений и предоставлять документы подтверждающие их.
- 12.2. Владелец сертификата ключа подписи и (или) лицо, ответственное за СКЗИ и уполномоченное для ведения электронного документооборота несет ответственность за сохранность и правильность эксплуатации СКЗИ и своих закрытых ключей ЭЦП.
- 12.3. В случае несвоевременного сообщения о факте компрометации ключей Владелец сертификата ключа подписи, допустивший компрометацию ключей, несет ответственность в полном объеме за ущерб, причиненный им другим Пользователям Системы.
- 12.4. Удостоверяющий Центр не несет ответственности в случае нарушения Участниками информационной системы положений настоящего Регламента.
- 12.5. Удостоверяющий Центр не несет ответственности перед Владельцами сертификатов ключей подписи (ключей шифрования) и (или) лицами, ответственными за СКЗИ и уполномоченными для ведения электронного документооборота, использующими сертификаты ключей подписи - для проверки подписи и шифрования сообщений, а также перед третьими лицами за любые убытки, потери, иной ущерб, связанный с использованием сертификатов ключей подписи, независимо от суммы заключенных с использованием сертификатов ключей подписи (ключа шифрования) сделок и совершения ими иных действий, за исключением случаев нарушения Удостоверяющим Центром обязательств, предусмотренных Регламентом и (или) действующим законодательством Российской Федерации.
- 12.6. Претензии к Удостоверяющему Центру ограничиваются указанием на несоответствие его действий настоящему Регламенту.
- 12.7. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту Участники информационной системы несут ответственность в

соответствии с Договором и действующим законодательством Российской Федерации.

- 12.8. Владелец сертификата ключа подписи и (или) лицо, ответственное за СКЗИ и ведения электронного документооборота несет ответственность за сохранность СКЗИ, своих закрытых ключей.

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ СТОРОН ПРИ НЕШТАТНЫХ СИТУАЦИЯХ, СВЯЗАННЫХ С ЭКСПЛУАТАЦИЕЙ СКЗИ

- 13.1. При возникновении непредвиденных ситуаций связанных с выходом из строя ключевого носителя, сбоев и отказов в работе СКЗИ, сбоев и отказов в работе средств электронной цифровой подписи и иных случаев, Владелец сертификата ключа подписи обязан:
- руководствоваться положениями и инструкциями эксплуатационной документации;
 - сообщить о возникшей ситуации в Удостоверяющий Центр;
 - выполнить указания специалистов технической поддержки Удостоверяющего Центра, касающиеся выхода из данной внештатной ситуации.

ПРОЧИЕ УСЛОВИЯ

- 14.1. Регламент может быть изменен и дополнен Удостоверяющим Центром в одностороннем порядке. При существенных изменениях Регламента Владельцы сертификатов ключей подписи уведомляются в срок не позднее, чем за 14 календарных дней до вступления в силу указанных изменений. Указанный в настоящем пункте срок уведомления может быть уменьшен Удостоверяющим центром в случае внесения изменений в Регламент в связи с изменением действующего законодательства Российской Федерации. Уведомления высылаются по адресу электронной почты, указанному в сертификате ключа подписи.
- 14.2. Удостоверяющий центр уведомляет всех лиц, присоединившихся к Регламенту, о внесении в него изменений путем публикации информационного письма, а также полного текста изменений на сайте Удостоверяющего центра в сети Интернет. Дополнительно к указанному способу уведомления Удостоверяющий центр по своему усмотрению может использовать иные способы информирования.
- 14.3. При незначительных изменениях и дополнениях Регламента Владельцы сертификатов могут не уведомляться.
- 14.4. Изменения в Регламент, вступившие в силу, распространяются на всех лиц, присоединившихся к Регламенту, независимо от даты присоединения к Регламенту (даты заключения Договора).
- 14.5. Участники информационной системы должны руководствоваться только последней актуальной версией Регламента.
- 14.6. Все приложения, изменения и дополнения являются неотъемлемой частью настоящего Регламента.

ПРИЛОЖЕНИЯ

- Приложение №1** Порядок разрешения конфликтных ситуаций, возникающих в ходе осуществления электронного документооборота.

- Приложение №2** Образец доверенности на право присутствия и получения сертификата ключа подписи.
- Приложение № 3** Образец заявления на аннулирование сертификата ключа подписи.
- Приложение № 4** Образец заявления на приостановление действия сертификата ключа подписи.
- Приложение № 5** Образец заявления на издание сертификата ключа подписи.
- Приложение № 6** Требования к программно-аппаратной части рабочей станции предназначенной для работы с СКЗИ.

ПОРЯДОК разрешения конфликтных ситуаций, возникающих при обмене электронными документами заверенными ЭЦП

1. Общие положения.

- 1.1. Разрешая конфликтные ситуации при нарушении процедур криптографической защиты информации и/или установлении авторства и/или подлинности электронных документов, заверенных ЭЦП, между Владельцем СКП и Пользователем системы исходят из того, что:
- в соответствии с действующим законодательством, документ в электронном виде, заверенный ЭЦП, является документом, имеющим юридическую силу, аналогичную бумажному документу, имеющему подпись и печать организации;
 - электронный документ порождает права и обязательства Владельца сертификата ключа подписи перед другим пользователем системы, если документ оформлен надлежащим образом, заверен ЭЦП и доставлен другому пользователю системы. При этом ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи, а сертификат ключа подписи действует.
 - подтверждением того, что электронный документ Владельца СКП принят Пользователем системы, является получение Владельцем СКП электронной квитанции о доставке сообщения или квитанции подписанной ЭЦП Пользователя системы.
 - Пользователь системы признает, что используемая в соответствии с настоящим Регламентом, система защиты информации, которая обеспечивается ЭЦП и шифрованием, достаточна для защиты информации от несанкционированного доступа, подтверждения целостности, подлинности и авторства электронных документов, а также разрешения конфликтных ситуаций по ним;
 - математические свойства алгоритма ЭЦП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р34.10-94 (или ГОСТ Р34.10-2001) и ГОСТ Р34.11-94, свидетельствуют о невозможности подделки значения ЭЦП любым лицом, не обладающим закрытым криптографическим ключом ЭЦП. Владелец СКП и Пользователь системы признают, что разбор конфликтной ситуации, в отношении авторства, целостности и подлинности электронного документа, заключается в доказательстве подписания конкретного электронного документа ЭЦП на основе конкретной ключевой пары.
- 1.2. В соответствии с настоящим порядком подлежат разрешению конфликтные ситуации двух типов:
- входящий электронный документ или ЭЦП данного документа некорректны (конфликтная ситуация типа А);
 - непризнание Владельцем СКП факта отправки, целостности и подлинности корректного электронного документа (конфликтная ситуация типа Б).

1.2.1. Порядок разрешения конфликтных ситуаций типа А.

Действия Владельца СКП и Пользователей в данной ситуации: .

Пользователь по телефону (или иным образом) запрашивает у Владельца СКП информацию о факте отправки электронного документа с ЭЦП, подлинность которого вызывает сомнения.

При получении подтверждения об отправке указанного документа, запрашивает повторное оформление и отправку данного документа.

Результатом повторной обработки (проверка ЭЦП) Пользователем полученного документа может быть:

А.1. Проверка ЭЦП, в повторно переданном документе, дала отрицательный результат.

В этом случае делается вывод о возможном нарушении действующих ключей электронной цифровой подписи, либо о неисправности программно-аппаратных средств одной из Сторон.

При этом необходимо:

- проверить сертификаты ключей подписи;
- штатными средствами в соответствии с эксплуатационной документацией проверить целостность и неизменность программного обеспечения СКЗИ. Переустановить его в случае необходимости.

Если положительный результат не достигнут, необходимо обратиться в Удостоверяющий Центр.

А.2. Повторная проверка дала положительный результат – электронный документ корректен, ЭЦП верна.

1.2.2. Порядок разрешения конфликтных ситуаций типа Б.

Если Владелец СКП приходит к выводу, что Пользователь системы ссылается на документ, исходящий от него, который им не отправлялся и/или его содержание изменено, то Владелец СКП немедленно извещает Удостоверяющий Центр о наличии такой конфликтной ситуации.

Удостоверяющий Центр в срок не более 5 рабочих дней с момента извещения о конфликтной ситуации формирует Экспертную (согласительную) комиссию для разрешения конфликтной ситуации, в состав которой входят представители Организатора Системы, Удостоверяющего Центра и Пользователи системы, вовлеченные в конфликтную ситуацию. Дополнительно могут привлекаться авторитетные, независимые специалисты в области криптографической защиты информации.

В ходе работы Экспертной комиссии рассматриваются все документы и материалы, относящиеся к предмету разногласий, и выполняется процедура проверки ЭЦП документа. Экспертной комиссии должны быть представлены следующие данные:

- электронный документ с ЭЦП, авторство которого оспаривается;
- архивные копии этого электронного документа с ЭЦП, переданные пользователями, вовлеченными в конфликтную ситуацию;
- сертификаты ключей подписи, изготовленные Удостоверяющим центром;
- дистрибутивы СКЗИ;
- ключевые носители.

При необходимости, Экспертная комиссия имеет право провести экспертизу ПЭВМ Сторон, вовлеченными в конфликтную ситуацию.

Экспертиза проводится на Автоматизированном рабочем месте Удостоверяющего Центра.

Экспертная комиссия подтверждает или опровергает факт отправки Владелецем СКП, авторство, целостность для документа, вызвавшего данную конфликтную ситуацию. Решение Экспертной комиссии оформляется в виде Протокола.

ДОВЕРЕННОСТЬ № _____

5

« _____ »⁶

ИНН _____⁷ ОКАТО _____⁸

юридический адрес: _____⁹

ДОВЕРЕННОСТЬ

город _____¹⁰, _____¹¹

на основании _____¹² « _____ »¹³, в лице _____¹⁴ _____¹⁵, действующего
на основании _____¹⁷ _____¹⁸, настоящей _____¹⁶ доверенностью _____¹⁵ уполномочивает

1. Предоставить в Удостоверяющий центр _____¹⁹ « _____ »²⁰ документы, необходимые для изготовления сертификата ключа подписи полномочного представителя _____²¹ « _____ »²² - Пользователя Удостоверяющего центра _____²³

⁵ Указывается организационно-правовая форма юридического лица согласно учредительным документам (например, открытое акционерное общество)

⁶ Указывается полное наименование юридического лица согласно учредительным документам

⁷ Указывается ИНН юридического лица

⁸ Указывается ОКАТО юридического лица

⁹ Указывается юридический адрес юридического лица

¹⁰ Указывается место составления доверенности

¹¹ Указывается дата составления доверенности (например, «третье июня две тысячи десятого года»)

¹² Указывается организационно-правовая форма юридического лица (например, ООО)

¹³ Указывается сокращенное наименование юридического лица согласно учредительным документам

¹⁴ Указывается должность лица, уполномоченного действовать от имени юридического лица (например, генерального директора)

¹⁵ Указывается фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица (например, Петрова Петра Петровича)

¹⁶ Указывается документ (документы) и его реквизиты, на основании которого (которых) указанное лицо уполномочено действовать от имени юридического лица (например, устава, доверенности от №).

¹⁷ Указывается фамилия, имя, отчество доверенного лица

¹⁸ Указывается документ, удостоверяющий личность доверенного лица, и его реквизиты

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

²⁰ Указывается полное наименование Удостоверяющего центра согласно учредительным документам

²¹ Указывается организационно-правовая форма (например, ООО) юридического лица

²² Указывается сокращенное наименование юридического лица согласно учредительным документам

²³ Указывается организационно-правовая форма (например, ООО) Удостоверяющего центра

«_____»²⁴, имеющего право участвовать в качестве участника размещения заказа на Отобранных электронных площадках.

2. Получить сертификат ключа подписи уполномоченного лица Удостоверяющего центра _____²⁵ «_____»²⁶ сформированные ключи подписи и сертификат ключа подписи Пользователя Удостоверяющего центра - _____²⁷

Доверенность выдана сроком на _____²⁸ без права передоверия.

(подпись) _____ (ФИО)

МП

²⁴ Указывается сокращенное наименование Удостоверяющего центра согласно учредительным документам

²⁵ Указывается организационно-правовая форма (например, ООО) Удостоверяющего центра

²⁶ Указывается сокращенное наименование Удостоверяющего центра согласно учредительным документам

²⁷ Указывается фамилия, имя, отчество Пользователя Удостоверяющего центра – участника размещения заказа

²⁸ 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

форму)

(полное наименование организации, включая организационно-правовую

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 | КРР=ИНН\КРР=КПП\ОГРН=ОГРН (ИНН организации \ КПП организации\ОГРН физического 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

Исполнительному директору ЗАО «АНК»
Пискареву Д.С.

192029, г.Санкт-Петербург, ул.Бабушкина, д.3,
оф.304б, 312

От _____
(Дол ж н о с т ь р у к о в о д и т е л я)

(Н а з в а н и е о р г а н и з а ц и и)

(Ф а м и л и я И . О .
р у к о в о д и т е л я)

(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.

(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.

« _____ »

Требования к программно-аппаратной части рабочей станции предназначенной для работы с СКЗИ.

1. Требования к Операционной Системе

Для работы с СКЗИ «КриптоПро CSP» 3.6. необходимо:

- Windows 32 (2000 Professional, 2000 Server, XP, 2003 Server, Vista, 2008 Server, Windows 7);
- Windows x64 (XP x64, 2003 Server x64, Vista x64, 2008 Server x64, Windows 7 x64 и Windows 2008 R2);

Для работы с СКЗИ «КриптоПро CSP» 3.0. необходимо:

- Windows 2000(с IE6)/XP/2003 x86;

Для работы с СКЗИ КриптоПро CSP 2.0.

- Windows 98\98SE\ME\2000 SP4;
- Windows NT 4.0 Service Pack 5 или выше;

2. Требования к аппаратному обеспечению

Для работы необходим персональный компьютер, снабжённый свободным портом USB (для USB-ключей) или (и) устройством для чтения смарт-карт (для смарт-карт).

3. Требования к Программному обеспечению

На персональном компьютере должно стоять следующему программное обеспечение:

- Драйверы к ключевому носителю в зависимости от производителя;
- Драйвер карт-ридера (если есть устройства чтения смарт-карт);
- «КриптоПро CSP» версии не ниже 2.0 build 2104;
- Модуль поддержки eToken /ruToken для «КриптоПро CSP».

4. Требования к ключевым носителям

В качестве ключевых носителей могут использоваться следующие устройства:

- Usb-брелоки :
 - eToken Pro;
 - eToken Pro Java;
 - eToken NG-OTP;
 - Rutoken, Rutoken S.
- Смарт-карты:
 - eToken Pro SC.

Использование Реестра или Магнитного диска для хранения ключей НЕ допустимо!