

**Министерство образования и науки Российской Федерации  
Томский государственный университета систем  
управления и радиозлектроники**

**Центр технологий безопасности**

**«УТВЕРЖДАЮ»**

**Руководитель ЦТБ ТУСУР**

**\_\_\_\_\_ А.А. Шелупанов**

# **РЕГЛАМЕНТ**

**Удостоверяющего центра  
Сибири**

**ЦТБ ТУСУР 2004**

## СОДЕРЖАНИЕ

Аннотация .....	4
1 Введение .....	4
1.1 Обзорная информация.....	4
1.2 Идентификация Регламента .....	4
1.3 Публикация Регламента .....	4
1.4 Область применения Регламента .....	5
1.5 Срок действия Регламента .....	5
1.6 Контактная информация .....	5
2 Общие положения .....	6
2.1 Назначение Удостоверяющего Центра Сибири .....	6
2.2 Услуги, предоставляемые Удостоверяющим Центром Сибири .....	6
2.3 Структура Системы .....	7
2.3.1 Центр сертификации УЦ Сибири:.....	7
2.3.2 Центр Регистрации УЦ Сибири: .....	7
2.3.3 Техническая служба УЦ Сибири:.....	7
2.3.4 Партнерские Центры Регистрации .....	8
2.4 Владельцы сертификатов открытых ключей ЭЦП .....	8
2.5 Пользователи сертификатов открытых ключей ЭЦП.....	8
2.6 Разрешение споров .....	8
2.7 Платность услуг .....	8
2.8 Ответственность.....	9
2.9 Прекращение деятельности .....	9
2.10 Порядок утверждения и внесения изменений в Регламент .....	9
3 Права и обязанности.....	10
3.1 Права Удостоверяющего Центра Сибири.....	10
3.2 Обязанности Центра Сертификации.....	10
3.3 Обязанности Центра Регистрации .....	11
3.4 Обязанности пользователей сертификатов .....	11
3.5 Обязанности владельцев закрытых ключей.....	11
3.6 Обязанности владельца сертификата открытого ключа .....	12
3.7 Обязанности пользователей сертификатов открытых ключей .....	12
4 Политика конфиденциальности.....	13
4.1 Типы конфиденциальной информации .....	13
4.2 Типы информации, не являющейся конфиденциальной.....	13
4.3 Исключительные полномочия официальных лиц .....	13
5 Процедура регистрации пользователей УЦ .....	14
5.1 Порядок регистрации .....	14
5.2 Аутентификация зарегистрированного пользователя .....	15
5.2.1 Очная аутентификация зарегистрированного пользователя .....	15
5.2.2 Удаленная аутентификация зарегистрированного пользователя .....	15
5.2.3 Аутентификация зарегистрированного пользователя по сертификату открытого ключа .....	15
5.2.4 Аутентификация зарегистрированного пользователя по паролю .....	15
5.3 Идентификация владельца сертификата открытого ключа .....	15
5.4 Приостановка действия и аннулирование сертификата .....	15

5.5	Список отозванных сертификатов .....	16
5.6	Действия при компрометации ключей .....	17
6	Дополнительные положения .....	17
6.1	Требования к средствам электронной цифровой подписи пользователей УЦ .....	17
6.2	Сроки действия закрытых ключей и сертификатов открытых ключей владельцев сертификатов открытых ключей .....	17
6.3	Архивирование документов .....	17
7	Структуры сертификатов и списков отозванных сертификатов .....	18
7.1	Структура сертификата открытого ключа, изготавливаемого Удостоверяющим Центром в электронной форме .....	18
7.1.1	Базовые поля сертификата открытого ключа .....	18
7.1.2	Дополнения сертификата .....	18
7.1.3	Объектные идентификаторы алгоритма .....	19
7.2	Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим Центром в электронной форме .....	19
7.2.1	Дополнения СОС .....	19
8	Юридические меры защиты информации .....	20
9	Термины и сокращения, используемые в регламенте .....	21
9.1	Сокращения .....	21
9.2	Термины и определения .....	21

## Аннотация

Центр технологий безопасности (ЦТБ) Томского государственного университета систем управления и радиоэлектроники (ТУСУР) действует как Удостоверяющий центр Сибири (УЦ Сибири) на основании приказа ректора ТУСУР. В своей деятельности как Удостоверяющий центр Сибири ЦТБ ТУСУР является законным представителем ТУСУР по всем юридическим вопросам.

## 1 Введение

### 1.1 Обзорная информация

Настоящий Регламент определяет механизмы и условия предоставления и использования услуг Удостоверяющего центра Томского университета систем управления и радиоэлектроники — Удостоверяющий Центр Сибири, включая обязанности пользователей (владельцев открытых ключей подписи), протоколы работы, принятые форматы данных, основные организационно-технические мероприятия.

### 1.2 Идентификация Регламента

Наименование документа: «Регламент работы Удостоверяющего Центра Сибири».

Версия: 1.1.

Дата: 11.08.2004г.

Объектный идентификатор: 1.2.643.3.19.0.

### 1.3 Публикация Регламента

Настоящий Регламент распространяется:

- 1 В электронной форме
  - из репозитория УЦ Сибири по адресу <https://www.udcs.ru>;
  - через E-mail от отправителя SA@udcs.ru.
- 2 В бумажной форме с почтового адреса  
**634050, г. Томск, пр. Ленина 40, ТУСУР КИБЭВС ЦТБ**
- 3 В бумажной форме в офисе  
**г. Томск, ул. Вершинина, 47, оф. 404а.**

Копии Регламента, предназначенные для распространения в электронной форме из репозитория УЦ Сибири, распространяются в виде двух файлов, один из которых содержит электронный образ Регламента в формате RTF, а другой — электронную цифровую подпись руководителя УЦ Сибири файла электронного образа Регламента, с использованием протокола HTTP(S) с использованием протокола обеспечения безопасности информации (SSL/TLS). Файл, содержащий электронную цифровую подпись руководителя Удостоверяющего Центра, имеет формат подписанных данных PKCS#7 Signed в кодировке Base64.

Копии Регламента, предназначенные для распространения в электронной форме через E-mail, распространяются в виде файла, содержащего электронный

образ Регламента в формате RTF, защищенного электронной цифровой подписью руководителя Удостоверяющего Центра с использованием S/MIME.

#### **1.4 Область применения Регламента**

Настоящий Регламент предназначен служить соглашением, налагающим обязательства по всем вовлеченным сторонам, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ Сибири.

Регламент применим при организации защищенного электронного документооборота, организованного при поддержке Центра технологий безопасности ТУСУР, в том числе и в интересах других юридических лиц (включая Министерство по налогам сборам России, Пенсионный фонд России, системы государственного заказа, органов государственной власти и т.д.).

#### **1.5 Срок действия Регламента**

Настоящий Регламент вступает в силу со дня его публикации.

Срок действия Регламента — 6 лет.

Если Удостоверяющий Центр официально не уведомит пользователей УЦ о прекращении действия Регламента, Регламент автоматически пролонгируется на следующие 6 лет.

Официальное уведомление о прекращении действия Регламента осуществляется способами, определенными в разделе публикации Регламента.

Копии уведомления, предназначенные для распространения в электронной форме из репозитория УЦ Сибири, распространяются с использованием протокола HTTP(S) с использованием протокола обеспечения безопасности информации (SSL/TLS).

Копии уведомления, предназначенные для распространения в электронной форме через E-mail, защищены электронной цифровой подписью с использованием S/MIME.

#### **1.6 Контактная информация**

Удостоверяющий центр Сибири

Почтовый адрес: 634050, г. Томск, пр. Ленина, 40, ТУСУР КИБЭВС ЦТБ УЦ

Адрес офиса: г. Томск, ул. Вершинина 47, оф. 404а

E-mail: [office@udcs.ru](mailto:office@udcs.ru)

Факс (3822) 413669

Контактный телефон Центра Сертификации УЦ Сибири (3822) 416000

E-mail Центра Сертификации УЦ Сибири: [sa@udcs.ru](mailto:sa@udcs.ru)

Контактный телефон Центра Регистрации УЦ: (3822) 413669

E-mail Центра Регистрации УЦ: [sr@udcs.ru](mailto:sr@udcs.ru)

Контактный телефон Технической Службы УЦ (3822) 412500

E-mail Технической Службы УЦ: [ts@udcs.ru](mailto:ts@udcs.ru)

## **2 Общие положения**

### **2.1 Назначение Удостоверяющего Центра Сибири**

Удостоверяющий Центр Сибири предназначен для обеспечения участников информационных систем средствами и спецификациями для использования сертификатов открытых ключей в целях обеспечения:

- применения электронной цифровой подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- аутентификации участников информационных систем в процессе взаимодействия;
- конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

### **2.2 Услуги, предоставляемые Удостоверяющим Центром Сибири**

В процессе своей деятельности Удостоверяющий Центр Сибири предоставляет потребителям (пользователям УЦ) следующие виды услуг:

1. внесение в реестр Удостоверяющего Центра Сибири регистрационной информации о пользователях УЦ;
2. изготовление сертификатов открытых ключей пользователей УЦ в электронной форме;
3. изготовление для владельцев сертификатов открытых ключей копии сертификатов открытых ключей на бумажном носителе;
4. формирование закрытых и открытых ключей, по обращениям пользователей УЦ, с записью их на ключевой носитель;
5. ведение реестра изготовленных сертификатов открытых ключей пользователей УЦ;
6. предоставление копий сертификатов открытых ключей в электронной форме, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ;
7. аннулирование (отзыв) сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
8. приостановление и возобновление действия сертификатов открытых ключей по обращениям владельцев сертификатов открытых ключей;
9. предоставление пользователям УЦ сведений об аннулированных и приостановленных сертификатах открытых ключей;
10. подтверждение подлинности электронных цифровых подписей в документах, представленных в электронной форме, по обращениям пользователей УЦ;
11. подтверждение подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах открытых ключей по обращениям пользователей УЦ;
12. распространение средств электронной цифровой подписи по обращениям пользователей УЦ;
13. другие виды услуг.

## **2.3 Структура Системы**

Удостоверяющий Центр Сибири состоит из следующих компонент:

- Центр Сертификации (ЦС);
- Центр Регистрации (ЦР);
- Техническая служба (ТС);
- Партнерские Центры Регистрации (ПЦР).

Все пользователи в данном регламенте разделяются на 2 категории:

- владельцы сертификатов открытых ключей ЭЦП (ВС);
- пользователи сертификатов открытых ключей ЭЦП (пользователи, не имеющие собственных сертификатов, но использующие сертификаты других пользователей для каких-либо целей).

### **2.3.1 Центр сертификации УЦ Сибири:**

- формирует сертификаты открытых ключей ЭЦП пользователей УЦ Сибири;
- формирует сертификаты открытых ключей ЭЦП уполномоченных лиц подчиненных УЦ (администраторов подчиненных УЦ);
- ведет базу данных действительных сертификатов открытых ключей ЭЦП;
- ведет базу данных недействительных сертификатов открытых ключей ЭЦП — список отозванных сертификатов (СОС);
- проводит отзыв сертификатов открытых ключей ЭЦП;
- ведет архив всех изготовленных в ЦС сертификатов.

### **2.3.2 Центр Регистрации УЦ Сибири:**

- регистрирует пользователей и подчиненных УЦ;
- ведет реестр зарегистрированных пользователей УЦ Сибири;
- обеспечивает взаимодействие пользователей и подчиненных УЦ с УЦ Сибири.

### **2.3.3 Техническая служба УЦ Сибири:**

- аннулирует (отзывает) сертификаты открытых ключей по обращениям владельцев сертификатов открытых ключей;
- приостанавливает и возобновляет действие сертификатов открытых ключей по обращению владельцев сертификатов открытых ключей;
- предоставляет пользователям УЦ сведений об аннулированных и приостановленных сертификатах открытых ключей;
- предоставляет копии сертификатов открытых ключей, находящихся в реестре изготовленных сертификатов, по запросам пользователей УЦ;
- проводит техническое обеспечение процедуры подтверждения ЭЦП в документах, представленных в электронной форме, по обращениям пользователей УЦ;
- организует и выполняет мероприятия по техническому сопровождению распространяемых средств электронной цифровой подписи и шифрования.
- распространяет средства электронной цифровой подписи и шифрования.

### **2.3.4 Партнерские Центры Регистрации**

Партнерские Центры Регистрации функционально входят в структуру УЦ Сибири, но образуются в организациях заключивших договор с УЦ Сибири по распространению услуг.

Партнерские Центры Регистрации выполняют задачи Центра Регистрации УЦ Сибири.

Партнерские Центры Регистрации предназначены для распространения услуг УЦ Сибири на территориях, отдаленных от главного офиса УЦ Сибири.

### **2.4 Владельцы сертификатов открытых ключей ЭЦП**

Владельцем сертификата может быть только **физическое лицо**.

Физическое лицо может представлять юридическое лицо при наличии доверенности, предоставляющей права данному физическому лицу пользоваться услугами, предоставляемыми Удостоверяющим Центром, и представлять юридическое лицо.

В случае, если физическое лицо действует от имени юридического лица на основании уставных документов, в Удостоверяющий Центр представляется специальный комплект документов согласно сферы деятельности.

В тех случаях, когда сертификаты требуются для работы каких-либо устройств или программных приложений, назначается ответственное лицо, на имя которого издается сертификат.

### **2.5 Пользователи сертификатов открытых ключей ЭЦП**

Пользователем сертификата может быть любое лицо, устройство или программное приложение.

### **2.6 Разрешение споров**

Сторонами в споре, в случае его возникновения, считаются Удостоверяющий Центр Сибири и пользователь УЦ.

При возникновении споров, стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, должны рассматриваться в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

### **2.7 Платность услуг**

Услуга Удостоверяющего Центра Сибири по предоставлению копий сертификатов открытых ключей в электронной форме, находящихся в реестре изготовленных сертификатов, предоставляется на безвозмездной основе.

Состав и стоимость предоставляемых дополнительных услуг определяется руководством ЦТБ ТУСУР.

## **2.8 Ответственность**

Удостоверяющий Центр Сибири не несет никакой ответственности в случае нарушения пользователями УЦ положений настоящего Регламента. Претензии к Удостоверяющему Центру ограничиваются указанием на несоответствие его действий настоящему Регламенту.

## **2.9 Прекращение деятельности**

Деятельность Удостоверяющего Центра Сибири может быть прекращена в порядке, установленном законодательством Российской Федерации.

В случае прекращения деятельности Удостоверяющего Центра реестр Удостоверяющего Центра, включающий реестр зарегистрированных пользователей УЦ, реестр изготовленных сертификатов открытых ключей, передаются в архив Уполномоченного Федерального органа.

## **2.10 Порядок утверждения и внесения изменений в Регламент**

Настоящий Регламент составляется в письменной форме и заверяется собственноручной подписью руководителя ЦТБ ТУСУР и печатью ЦТБ ТУСУР (или руководителем Удостоверяющего Центра Сибири и печатью Удостоверяющего Центра Сибири).

Изменения в Регламент вносятся путем составления Дополнительного Соглашения к Регламенту или выпуска новой версии Регламента.

Изменению не подлежат положения настоящего Регламента, прямо или косвенно ущемляющие права пользователей услуг Удостоверяющего Центра.

Утверждение и публикация дополнительных соглашений к Регламенту осуществляется в порядке, соответствующему порядку утверждения и публикации Регламента.

Дополнения к Регламенту по организации конкретных защищенных систем электронного документооборота являются самостоятельными документами и утверждаются организаторами защищенных систем электронного документооборота при условии выполнения данного Регламента и не противоречия ему.

### **3 Права и обязанности**

#### **3.1 Права Удостоверяющего Центра Сибири**

Удостоверяющий Центр Сибири имеет право:

1. Предоставлять копии сертификатов открытых ключей в электронной форме, находящихся в реестре Удостоверяющего Центра, всем лицам, обратившимся за копиями в Удостоверяющий Центр;
2. Не проводить регистрацию лиц, обратившихся по вопросу предоставления копий сертификатов открытых ключей в электронной форме, находящихся в реестре Удостоверяющего Центра;
3. Отказать в предоставлении услуг по регистрации пользователям УЦ, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;
4. Отказать в изготовлении ключей не зарегистрированным пользователям УЦ, подавшим заявление на изготовление ключей, без предоставления информации о причинах отказа;
5. Отказать в изготовлении сертификата открытого ключа зарегистрированным пользователям УЦ, подавшим заявление на изготовление сертификата открытого ключа, с указанием причин отказа;
6. Отказать в аннулировании (отзыве) сертификата открытого ключа владельцу сертификата, подавшим заявление на аннулирование (отзыв) сертификата, в случае если истек установленный срок действия закрытого ключа, соответствующему открытому ключу в сертификате;
7. Отказать в приостановлении или возобновлении действия сертификата открытого ключа владельцу сертификата, подавшему заявление на приостановлении или возобновлении действия сертификата, в случае если истек установленный срок действия закрытого ключа, соответствующему открытому ключу в сертификате;
8. Аннулировать (отозвать) сертификат открытого ключа пользователя УЦ в случае установленного факта компрометации соответствующего закрытого ключа, с уведомлением владельца аннулированного (отозванного) сертификата открытого ключа и указанием обоснованных причин;
9. Приостановить действие сертификата открытого ключа пользователя УЦ, с уведомлением владельца приостановленного сертификата открытого ключа и указанием обоснованных причин.

УЦ не несет никакой ответственности в случае нарушения пользователями положений данного Регламента. Претензии к УЦ ограничиваются указанием на несоответствие его действий данному Регламенту.

#### **3.2 Обязанности Центра Сертификации**

В своей деятельности ЦС должен руководствоваться данным Регламентом, постановлениями органов государственной власти РФ, законом РФ «Об электронной цифровой подписи» и другими законами РФ. ЦС должен гарантировать, что все ЦР, действующие от его имени, удовлетворяют соответствующим положениям данного Регламента касательно деятельности ЦР. ЦС должен принимать все допустимые меры для ознакомления владельцев и пользователей сертификатов с их правами и

обязанностями в плане управления ключевой информацией, сертификатами и программно-аппаратным обеспечением, используемым при взаимодействии с УЦ.

ЦС обязан:

- публиковать данный Регламент;
- располагать механизмами и процедурами, позволяющими гарантировать, что все ЦР и пользователи сознательно согласны следовать положениям данного Регламента;
- гарантировать, что собственные службы издания и отзыва сертификатов, издания списков отозванных сертификатов согласуются с данным Регламентом.

### **3.3 Обязанности Центра Регистрации**

В своей деятельности ЦР должен руководствоваться данным Регламентом.

ЦР отвечает за доведение до сведения пользователей всей информации, касающейся прав и обязанностей ЦС, ЦР, владельцев и пользователей сертификатов, содержащейся в данном Регламенте.

### **3.4 Обязанности пользователей сертификатов**

Лица, проходящие процедуру регистрации в реестре Удостоверяющего Центра, обязаны представить регистрационную и идентифицирующую информацию в объеме, определенном положениями настоящего Регламента. Лица, проходящие процедуру регистрации в распределенном режиме, обязаны хранить в тайне предоставленный пароль для аутентификации по паролю в течение срока действия пароля.

Владелец сертификата обязан выразить согласие с положениями данного Регламента и следовать ему.

Перед тем как использовать сертификат пользователь сертификата должен удостовериться, что назначение сертификата соответствует предполагаемому использованию.

Перед тем как использовать сертификат, пользователь сертификата должен проверить его действительность согласно официальной спецификации сертификатов X.509 (RFC 2459) с помощью сертифицированных программных средств, обеспечивающих выполнение такой проверки.

### **3.5 Обязанности владельцев закрытых ключей**

Владелец закрытого ключа обязан:

- хранить в тайне закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;
- не использовать для электронной цифровой подписи закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее другими лицами;
- использовать закрытый ключ только для целей, разрешенных соответствующими областями использования, определенными в сертификате соответствующего открытого ключа согласно настоящему Регламенту.

### **3.6 Обязанности владельца сертификата открытого ключа**

Владелец сертификата открытого ключа, изданного Удостоверяющим Центром, обязан:

- использовать сертификат открытого ключа только для целей, разрешенных соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту;
- немедленно обратиться в Удостоверяющий Центр с заявлением на аннулирование (отзыв) сертификата открытого ключа в случае, если ему известно, что эти ключи используются или использовались ранее другими лицами.

### **3.7 Обязанности пользователей сертификатов открытых ключей**

Перед тем как использовать сертификат открытого ключа, изготовленный Удостоверяющим Центром, пользователь сертификата (пользователь, не являющийся его владельцем) должен удостовериться, что назначение сертификата, определенное соответствующими областями использования, определенными в сертификате согласно настоящему Регламенту, соответствует предполагаемому использованию.

## **4 Политика конфиденциальности**

### **4.1 Типы конфиденциальной информации**

Закрытый ключ владельца сертификата открытого ключа является конфиденциальной информацией данного пользователя УЦ. Удостоверяющий Центр не депонирует и не архивирует закрытые ключи.

Персональная и корпоративная информация пользователей УЦ, содержащаяся в Удостоверяющем Центре, не подлежащая непосредственной рассылке в качестве части сертификата открытого ключа, списка отозванных сертификатов, считается конфиденциальной и не публикуется.

Информация, хранящаяся в журналах аудита Удостоверяющего Центра, считается конфиденциальной и не подлежит разглашению.

Отчетные материалы по выполненным проверкам деятельности Удостоверяющего Центра являются конфиденциальными, за исключением заключения по результатам проверок, публикуемого в соответствии с настоящим Регламентом.

### **4.2 Типы информации, не являющейся конфиденциальной**

Информация, не являющейся конфиденциальной информацией, является открытой информацией.

Открытая информация может публиковаться по решению Удостоверяющего Центра Сибири. Место, способ и время публикации также определяется решением Удостоверяющего Центра Сибири.

Информация, включаемая в сертификаты открытых ключей пользователей УЦ и списки отозванных сертификатов, издаваемые Удостоверяющим Центром, не считается конфиденциальной.

Также не считается конфиденциальной информация о настоящем Регламенте.

### **4.3 Исключительные полномочия официальных лиц**

Удостоверяющий Центр не должен раскрывать информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам за исключением случаев:

- определенных в настоящем Регламенте;
- требующих раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.

## **5 Процедура регистрации пользователей УЦ**

Под регистрацией пользователей УЦ понимается внесение регистрационной информации о пользователях УЦ в реестр Удостоверяющего Центра.

Процедура регистрации пользователей УЦ применяется в отношении физических лиц, обращающихся к услугам Удостоверяющего Центра в части изготовления сертификатов открытых ключей пользователей УЦ и/или формирования закрытых и открытых ключей пользователей УЦ с записью их на ключевой носитель.

Идентификация пользователя выполняется в процессе его регистрации в качестве зарегистрированного пользователя УЦ.

Результатом идентификации является присвоение пользователю УЦ идентификатора и занесение идентификатора в Реестр зарегистрированных пользователей Удостоверяющего Центра.

### **5.1 Порядок регистрации**

Для регистрации Пользователей УЦ Пользователь заключает Договор с Удостоверяющим центром Сибири и производит оплату.

Руководитель Пользователя в соответствии с Договором представляет в Центр Регистрации комплект документов и заявку на подключение (Приложение №1), содержащую:

- данные на сотрудника Пользователя, ответственного за СКЗИ;
- список сотрудников Пользователя, которым необходимо изготовить криптографические ключи,

Администратор Удостоверяющего центра (УЦ) согласует с Пользователем, график работ.

В соответствии с согласованным графиком сотрудники Пользователя лично или их доверенные лица (при оформленной доверенности Приложение №2):

- прибывают в Центр регистрации УЦ;
- регистрируются Администратором УЦ;
- получают СКЗИ в технической службе УЦ Сибири
- расписываются в журнале о получении СКЗИ;
- генерируют криптографические ключи самостоятельно или получают изготовленные в их присутствии ключи и сертификаты;
- расписываются в журнале о получении криптографических ключей и сертификатах (Приложение №3);
- получают сертификат УЦ;
- получают список отозванных сертификатов (СОС);
- получают пароль для связи на случай компрометации ключей;
- инструктируются Администратором УЦ правилам работы с СКЗИ.

Пользователь в соответствии с документацией полученной в УЦ Сибири самостоятельно (или сотрудником УЦ в соответствии с договором) производит все необходимые работы по установке и настройке СКЗИ на своем рабочем месте.

## **5.2 Аутентификация зарегистрированного пользователя**

### **5.2.1 Очная аутентификация зарегистрированного пользователя**

Очная аутентификация зарегистрированного пользователя УЦ выполняется по паспорту или другому документу удостоверяющего личность, предъявляемого лично.

### **5.2.2 Удаленная аутентификация зарегистрированного пользователя**

Удаленная аутентификация зарегистрированного пользователя УЦ предназначена для идентификации зарегистрированного пользователя УЦ по средствам телефонной связи. Удаленная аутентификация зарегистрированного пользователя УЦ выполняется по ключевой фразе, определенной пользователем в заявлении на регистрацию.

Лицо, проходящее процедуру удаленной аутентификации должен сообщить свои идентификационные данные и, по запросу сотрудника УЦ, назвать ключевую фразу.

### **5.2.3 Аутентификация зарегистрированного пользователя по сертификату открытого ключа**

Аутентификация зарегистрированного пользователя УЦ по сертификату открытого ключа выполняется путем выполнения процедуры подтверждения электронной цифровой подписи с использованием сертификата открытого ключа.

### **5.2.4 Аутентификация зарегистрированного пользователя по паролю**

Аутентификация зарегистрированного пользователя УЦ по паролю выполняется путем сопоставления предъявленного зарегистрированным пользователем УЦ пароля с учетной информацией хранимой в Реестре зарегистрированных пользователей Удостоверяющего Центра.

Действие пароля начинается с момента его предоставления пользователю УЦ.

Срок действия пароля составляет 30 календарных суток или ограничивается по времени моментом установки выпущенного Удостоверяющим Центром сертификата открытого ключа на рабочее место зарегистрированного пользователя УЦ (что наступит раньше).

## **5.3 Идентификация владельца сертификата открытого ключа**

Владелец сертификата открытого ключа идентифицируется по значениям атрибутов поля Subject сертификата открытого ключа.

## **5.4 Приостановка действия и аннулирование сертификата**

Сертификат должен быть отозван, если информация в нем более не может пользоваться доверием. Причины отзыва сертификата:

- временное отстранение владельца сертификата от выполнения служебных обязанностей;
- компрометация или подозрение на компрометацию закрытого ключа;
- изменение идентифицирующей информации или атрибутов в сертификате пользователя до истечения срока действия сертификата;

- увольнение владельца сертификата;
  - невыполнение владельцем сертификата своих обязательств, изложенных в данном Регламенте или дополнительных соглашениях.  
Запрос на отзыв сертификата может быть сделан только:
    - владельцем сертификата;
    - Центром Сертификации;
    - Центром Регистрации.
- Запросы на отзыв должны содержать:
- информацию, позволяющую идентифицировать сертификат, который следует отозвать;
  - причину отзыва;
  - данные, позволяющие проверить аутентичность запроса.

По принятии и согласии с запросом на отзыв сертификата, ЦС должен отозвать сертификат. Аутентифицированный запрос на отзыв и результат действий, предпринятых ЦС или ЦР, должны быть сохранены в архиве.

ЦС должен включить данные об отозванном сертификате в очередной СОС.

Любое действие, являющееся реакцией на запрос на отзыв сертификата, должно быть произведено в течение двух рабочих дней с момента приема отзыва.

ЦС может приостановить действие сертификата в случае временного прекращения выполнения владельцем своих обязанностей.

Запросы на приостановление действия должны содержать:

- информацию, позволяющую идентифицировать сертификат, действие которого следует приостановить;
- причину приостановления действия;
- данные, позволяющие проверить аутентичность запроса.

По принятии и согласии с запросом на приостановление действия сертификата, ЦС должен приостановить действие сертификата. Аутентифицированный запрос на приостановление действия и результат действий, предпринятых ЦС или ЦР, должны быть сохранены в архиве.

ЦС должен включить данные о сертификате в очередной СОС.

Период времени, на который приостанавливается действие сертификата, должен быть указан в запросе на приостановление действия сертификата.

### **5.5 Список отозванных сертификатов**

Список отозванных сертификатов содержит список отозванных или приостановленных сертификатов.

Перед использованием сертификата пользователь обязан:

- проверить статус всех сертификатов в цепочке проверки сертификата на предмет отсутствия их в текущем СОС;
- проверить аутентичность и целостность СОС.

Если получение текущего СОС по той или иной причине является временно невыполнимой задачей, то пользователь должен отказаться от использования сертификата.

## **5.6 Действия при компрометации ключей**

В случае компрометации или подозрения на компрометацию ключа ЦС, используемого для подписи сертификатов и СОС, ЦС обязан немедленно оповестить об этом всех пользователей.

В любом случае компрометации ключа пользователь обязан немедленно оповестить об этом ЦС, издавший сертификат, или соответствующий ЦР.

## **6 Дополнительные положения**

### **6.1 Требования к средствам электронной цифровой подписи пользователей УЦ**

Средство электронной цифровой подписи должно обеспечивать выполнение следующих процедур:

- генерацию закрытых и открытых ключей;
- формирование электронной цифровой подписи;
- проверку электронной цифровой подписи. Средство электронной цифровой подписи должно обеспечивать выполнение мер защиты закрытых ключей.

Средства криптографической защиты информации должны иметь режимы работы, совместимые с нормальными режимами работы программного обеспечения Удостоверяющего центра Сибири.

### **6.2 Сроки действия закрытых ключей и сертификатов открытых ключей владельцев сертификатов открытых ключей**

Срок действия ключей и сертификатов:

- закрытый ключ ЦС (используемый для подписи сертификатов и СОС) - 6 лет;
- открытый ключ и сертификат ЦС - 6 лет;
- другие закрытые и открытые ключи и сертификаты ЦС и ЦР – 1 год;
- закрытые и открытые ключи и сертификаты пользователей - 1 год;

### **6.3 Архивирование документов**

Архивированию подлежат, как минимум, следующие данные:

- сертификаты;
- заявки на получение сертификатов, сообщения о признании сертификатов;
- идентифицирующая и аутентифицирующая информация, предоставленная пользователями.

Все данные должны содержаться в архиве на протяжении 5 лет.

Защита архивируемой информации должна осуществляться методами физического обеспечения безопасности или комбинацией методов физической и криптографической защиты.

Все резервные файлы архивируемой информации должны храниться в защищенном и географически удаленном месте.

Только уполномоченный персонал имеет доступ к архивной информации. Процедуры получения и проверки архивной информации не регламентируются.

## 7 Структуры сертификатов и списков отозванных сертификатов

### 7.1 Структура сертификата открытого ключа, изготавливаемого Удостоверяющим Центром в электронной форме

Удостоверяющий Центр Сибири издает сертификаты открытых ключей пользователей УЦ и уполномоченных лиц Удостоверяющего Центра Сибири в электронной форме (далее по тексту раздела - сертификаты открытых ключей) формата X.509 версии 3.

#### 7.1.1 Базовые поля сертификата открытого ключа

Сертификаты открытых ключей содержат следующие базовые поля X.509:

Signature:	электронная цифровая подпись уполномоченного лица Удостоверяющего центра
Issuer:	идентифицирующие данные уполномоченного лица Удостоверяющего центра
Validity:	даты начала и окончания срока действия сертификата
Subject:	идентифицирующие данные владельца сертификата открытого ключа
SubjectPublicKeyInformation	идентификатор алгоритма средства электронной цифровой подписи, с которыми используется данный открытый ключ, значение открытого ключа
Version:	версия сертификата формата X.509 - версия 3
SerialNumber:	уникальный серийный (регистрационный) номер сертификата в реестре сертификатов открытых ключей Удостоверяющего центра Сибири

#### 7.1.2 Дополнения сертификата

Сертификаты открытых ключей содержат следующие дополнения:

AuthorityKeyIdentifier	идентификатор ключа уполномоченного лица Удостоверяющего Центра Сибири
SubjectKeyIdentifier	идентификатор ключа владельца сертификата
ExtendedKeyUsage	Область (области) использования ключа, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение
CRLDistributionPoint	точка распространения списка аннулированных (отозванных) сертификатов открытых ключей, изданных Удостоверяющим Центром Сибири
KeyUsage	Назначение ключа

### **7.1.3 Объектные идентификаторы алгоритма**

Удостоверяющий Центр поддерживает следующие алгоритмы:

ГОСТ Р 34.10-94	1.2.643.2.2.20
Диффи-Хеллмана	1.2.643.2.2.99
ГОСТ Р 34.10-2001	1.2.643.2.2.19
Диффи-Хеллмана	1.2.643.2.2.99
ГОСТ Р 34.11-94	1.2.643.2.2.9
ГОСТ 28147-89	1.2.643.2.2.21

### **7.2 Структура списка отозванных сертификатов, изготавливаемого Удостоверяющим Центром в электронной форме**

Удостоверяющий Центр Сибири издает списки отозванных сертификатов открытых ключей пользователей УЦ и уполномоченного лица Удостоверяющего Центра Сибири в электронной форме (далее по тексту раздела СОС) формата X.509 версии 2.

#### **7.2.1 Дополнения СОС**

Удостоверяющий Центр Сибири использует следующие дополнения:

Authority Key Identifier	идентификатор ключа уполномоченного лица Удостоверяющего Центра Сибири
--------------------------	---

## **8 Юридические меры защиты информации**

Центр Технологий Безопасности ТУСУР имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг.

Системы безопасности и защиты информации Удостоверяющего Центра Сибири функционируют в рамках режима ТУСУР и систем защиты информации ЦТБ ТУСУР.

Все меры по защите информации в Удостоверяющем Центре Сибири введены в действие распоряжением руководителя ЦТБ ТУСУР

Для обеспечения деятельности Удостоверяющий Центр Сибири использует средства электронной цифровой подписи и криптографической защиты информации, сертифицированные в соответствии с действующим законодательством Российской Федерации.

Исключительные имущественные права на информационные ресурсы Удостоверяющего Центра Сибири находятся в собственности ЦТБ ТУСУР.

Пользователям УЦ Сибири предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, изготавливаемые Удостоверяющим Центром Сибири в объеме прав согласно разделу 3.1 настоящего Регламента.

## 9 Термины и сокращения, используемые в регламенте

### 9.1 Сокращения

АС	Автоматизированная система;
ЗЭД	Защищенный электронный документооборот;
РФ	Российская Федерация;
СОС	Список отозванных сертификатов;
ТУСУР	Томский государственный университет систем управления и радиоэлектроники;
УЦ	Удостоверяющий Центр;
ЦР	Центр Регистрации;
ЦС	Центр Сертификации;
ЦТБ ТУСУР	Центр технологий безопасности ТУСУР;
ЭД	Электронный документооборот;
ЭЦП	Электронная цифровая подпись.

### 9.2 Термины и определения

**Авторство документа** — принадлежность документа одному из участников (Пользователю) системы электронного документооборота (Система). Авторство документа определяется путем аутентификации содержащейся в нем информации.

**Аутентификация информации** — установление 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 и проверкой правильности электронной цифровой подписи (ЭЦП) для электронных документов при использовании сертифицированных ФСБ (ФАПСИ) средств криптографической защиты информации (СКЗИ).

**Владелец сертификата ключа** — физическое лицо, на имя которого выдан сертификат ключа и которое владеет соответствующим закрытым криптографическим ключом.

**Пользователь** — юридическое или физическое лицо, участник информационного обмена электронными документами, заключивший с Удостоверяющим Центром Сибири Договор, зарегистрированный в ЦР и признающий данный Регламент.

**Внеплановая смена ключей** — смена ключей в соответствии с Документацией на СКЗИ, вызванная компрометацией ключей.

**Договор** — Договор заключенный между Пользователем и Удостоверяющим Центром Сибири.

**Запрос на сертификат** — Сообщение, содержащее необходимую информацию для получения сертификата.

**Запрос на отзыв сертификата** — Сообщение, содержащее необходимую информацию для отзыва сертификата.

**Зарегистрированный (сертифицированный) открытый ключ** — открытый ключ, подписанный ЭЦП Удостоверяющего Центра, и подтвержденный сертификатом открытого ключа.

**Идентификация** — Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Ключевая пара** — Открытый и закрытый ключи.

**Ключевой носитель** — Носитель, содержащий один или несколько ключей.

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

- утрата ключевых дискет или иных носителей ключа;
- утрата ключевых дискет или иных носителей ключа с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
- доступ посторонних лиц к ключевой информации.

**Конфиденциальность информации** - субъективно определяемая характеристика информации, означающая необходимость введения ограничений на круг лиц, имеющих к ней доступ.

**Конфиденциальная информация** — информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, а также настоящим Регламентом.

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

**Корректный электронный документ** — электронный документ, прошедший процедуру проверки ЭЦП с подтверждением ее правильности и не имеющий искажений в тексте сообщения, не позволяющих понять его смысл.

**Криптографическая защита** — защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

**Криптографический ключ (ключ)** — параметр шифра или его значение, определяющее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

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

**Несанкционированный доступ к информации** — доступ к информации лиц, не имеющих на то полномочий.

**Обработка информации** — создание, хранение, передача, прием, преобразование и отображение информации.

**Открытый ключ 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 Пользователя 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.

**Плановая смена ключей** — смена ключей, не вызванная компрометацией ключей, в соответствии с Документацией на СКЗИ, с периодичностью согласованной с Пользователем, но не превышающей 1 (одного) года.

**Подтверждение подлинности электронной цифровой подписи в электронном документе** — положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи 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.

**Расшифрование** — процесс преобразования шифрованной информации в открытую при помощи шифра.

**Сертификат открытого ключа** — документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, которые включают в себя открытый ключ (ЭЦП и/или шифрования) и которые выдаются Удостоверяющим центром участнику информационной системы для подтверждения подлинности открытого ключа и идентификации владельца сертификата открытого ключа;

**Секретные (закрытые) ключи** — криптографические ключи, которые хранятся Пользователями Системы в тайне. Секретные ключи используются для шифрования документов и формирования ЭЦП Пользователя.

**Список отозванных сертификатов** — Созданный УЦ список сертификатов, отозванных до окончания срока их действия.

**Средство электронной цифровой подписи** — Аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи;
- подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;
- создание закрытых и открытых ключей электронных цифровых подписей.

**Управление ключами** — создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение а также выдача и отзыв сертификатов открытых ключей в соответствии с политикой безопасности.

**Шифрование** — процесс преобразования открытой информации с целью сохранения ее в тайне от посторонних лиц при помощи некоторого алгоритма, называемого шифром.

**Шифр** — совокупность обратимых преобразований множества возможных открытых данных на множество возможных шифрованных данных, осуществляемых по определенным правилам с применением ключей.

**Электронный документ** — документ, в котором информация представлена в электронно-цифровой форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия.

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

**Форма заявки Пользователя на изготовление ключей и сертификатов**

**Руководителю «УДОСТОВЕРЯЮЩИЙ ЦЕНТР СИБИРИ»  
Шелупанову А.А.**

**От (руководителя организации,  
Фамилия, Имя, Отчество,  
адрес организации, контактные данные)**

Прошу, Вас в соответствии с Договором № \_\_\_\_\_ от «\_\_\_» \_\_\_\_\_ 200\_\_ г.  
изготовить ключи и сертификат ЭЦП (ЭЦП и шифрования, только шифрования) для  
сотрудника(ов) нашей организации:

(Список сотрудников организации, которым необходимо изготовить  
криптографические ключи)

- Ф.И.О., должность \_\_\_\_\_
- ЭЦП будет использоваться для \_\_\_\_\_
- телефон/факс \_\_\_\_\_
- e-mail \_\_\_\_\_
- тип компьютера, операционная система. \_\_\_\_\_

- рабочее место расположено по адресу \_\_\_\_\_

Ответственным за СКЗИ и Систему назначен:

- Ф.И.О., должность \_\_\_\_\_
- телефон/факс \_\_\_\_\_
- e-mail \_\_\_\_\_

Помещения, режим эксплуатации программного обеспечения и  
персональных компьютеров на которые будут установлены СКЗИ, удовлетворяют  
требованиям ФАПСИ по обеспечению безопасности информации при ее защите по  
уровню "С" (на уровне потребителя), изложенным в Приложении №5 Регламента

Руководитель \_\_\_\_\_ / Фамилия И.О. /  
М.П. " \_\_\_\_\_ " \_\_\_\_\_ 200\_\_ г.

Доверенность № \_\_\_\_\_

Дата выдачи « \_\_\_\_\_ » \_\_\_\_\_ 200 г.

Доверенность действительна по « \_\_\_\_\_ » \_\_\_\_\_ 200 г.

**Я, (Фамилия Имя Отчество доверителя)**

- Должность \_\_\_\_\_
- Паспорт: Серия \_\_\_\_\_ № \_\_\_\_\_  
Кем выдан \_\_\_\_\_  
Дата выдачи « \_\_\_\_\_ » \_\_\_\_\_ г.

**доверяю (Фамилия Имя Отчество доверенного лица)**

- Должность \_\_\_\_\_
- Паспорт: Серия \_\_\_\_\_ № \_\_\_\_\_  
Кем выдан \_\_\_\_\_  
Дата выдачи « \_\_\_\_\_ » \_\_\_\_\_ г.

**ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:**

- вместо меня присутствовать при изготовлении моих криптографических ключей (ЭЦП, шифрования) и сертификатов;
- получить ключевые носители;
- получить сертификаты открытых ключей;
- расписываться за меня в регистрационных журналах;
- \_\_\_\_\_ другие полномочия \_\_\_\_\_.

Подпись доверителя \_\_\_\_\_ (Ф.И.О.)

Подпись лица, получившего доверенность \_\_\_\_\_ (Ф.И.О.)

**УДОСТОВЕРЯЮ**

(наименование организации, должность руководителя организации)

\_\_\_\_\_ (Фамилия И.О.)

М.П.

" \_\_\_\_\_ " \_\_\_\_\_ 200\_\_ г.

### Образец Сертификата открытого ключа

#### Центр технологий безопасности ТУСУР «УДОСТОВЕРЯЮЩИЙ ЦЕНТР СИБИРИ»

Сертификат выдан по стандарту X.509

**Этот сертификат:**

Подтверждает удаленному компьютеру идентификацию вашего компьютера  
Защищает сообщения электронной почты

**Кому выдан:**

Иванов Иван Иванович

**Кем выдан:**

ЦТБ ТУСУР «Удостоверяющий центр Сибири»

Действителен с 01 июня 2004 г. 12:17:18 по 01 июня 2004 г. 12:27:18

**Версия:** 3 (0x2)

**Серийный номер:**

1A57 159D 0000 0000 001A

**Алгоритм подписи:**

Название:

ГОСТ Р 34.11/34.10-94

Идентификатор:

1.2.643.2.2.4

Параметры:

0500

**Издатель:**

CN = UC

O = UC

L = Saint-Petersburg

C = RU

E = svtel@atcom.spb.ru

**Срок действия:**

Действителен с:

10 июня 2002 г. 20:17:18

Действителен по:

10 июня 2004 г. 20:27:18

**Субъект:**

CN = Иванов Иван Иванович

OU = Директор

O = названия организации Пользователя

E = svtel@atcom.spb.ru

**Открытый ключ:**

Алгоритм открытого ключа:

Название:

ГОСТ Р 34.10-94

Идентификатор:

1.2.643.2.2.20

Параметры:

3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01

Значение:

0481 807D 3F00 E5EA D35D 92D6 42E7 B86F 2817  
E7E8 8EA9 7E5C 1405 6149 B93F 1D18 971F 59EC  
B9F7 B5A2 16C0 C846 B5A4 DAB8 7472 80EB 5ADE  
8260 1B55 D4BA 9969 179A DDE9 5EF9 8A2C 2938  
25AA CAD3 C5F0 3C8B BC5A 4C3A 0693 221B C673  
37B7 C51D 946C 9148 44D6 6DAF B9E7 8C2E 6F80  
59F5 19B8 A834 79A5 AC56 E25B 8FCF C610 2922

C951 5383 9D

**Расширения X.509**

1. Расширение 2.5.29.15 (критическое)

Название:

Использование ключа

Значение:

Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных(F0)

2. Расширение 2.5.29.37

Название:

Улучшенный ключ

Значение:

Защищенная электронная почта(1.3.6.1.5.5.7.3.4)

Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)

3. Расширение 2.5.29.14

Название:

Идентификатор ключа субъекта

Значение:

592F 42BC 2F49 9119 FE33 B462 3209 DAE3 603D 0F4A

4. Расширение 2.5.29.35

Название:

Идентификатор ключа центра сертификатов

Значение:

Идентификатор ключа=39FB 989D 4390 1EA8 17DE 665D C2BE 5A4F 3576 CB51

Поставщик сертификата:

Адрес каталога:

CN=UC

O=UC

L=Saint-Petersburg

C=RU

E=svtel@atcom.spb.ru

Серийный номер сертификата=2CC8 B590 37F0 8380 44D8 DB15 ECC9 BA79

5. Расширение 2.5.29.31

Название:

Точки распространения списков отзыва (CRL)

Значение:

[1]Точка распределения списка отзыва (CRL)

Имя точки распространения:

Полное имя:

URL=http://sertserver/certsrv/certcrl.crl

**Подпись:**

Алгоритм подписи:

Название:

ГОСТ Р 34.11/34.10-94

Идентификатор:

1.2.643.2.2.4

Параметры:

0500

Значение:

EE23 1505 75E6 5E02 3262 8AA6 3657 2083 DDF9

40B4 02C2 8FC4 C90B 5170 814E 9A3C 1D0E A25E

B152 12AD B57A 199D 71F4 5D62 9DBB 2432 FD10

2B22 C985 9B4C 2FB4 6600

**Владелец сертификата**

**Администратор  
центра**

**Удостоверяющего  
центра**

\_\_\_\_\_ Фамилия И.О.

**Регламент Удостоверяющего Центра Сибири**

---

“ \_\_\_ ” \_\_\_\_\_ 200\_г.

\_\_\_\_\_ Фамилия И.О.

“ \_\_\_ ” \_\_\_\_\_ 200\_г.  
М.П.

Приложение № 4  
к Регламенту  
УТВЕРЖДАЮ  
Руководитель  
«УДОСТОВЕРЯЮЩИЙ ЦЕНТР СИБИРИ»  
Шелупанов А.А.

«\_\_\_»\_\_\_\_\_ 200\_г.

М.П.

**Акт  
Приема-передачи СКЗИ в эксплуатацию**

"\_\_\_"\_\_\_\_\_ 200\_г.

г. Томск.

Настоящий акт составлен

\_\_\_\_\_ (наименование Пользователя)

\_\_\_\_\_ (должность, фамилия, имя, отчество Пользователя)

и

\_\_\_\_\_ (фамилия, имя, отчество сотрудника "Удостоверяющего центра Сибири")

о том, что УЦ Сибири, в соответствии с Договором №\_\_\_ от «\_\_\_» \_\_\_\_\_ 200\_\_ г. выполнил следующие работы:

1. передал Пользователю СКЗИ рег. №\_\_\_\_\_ с эксплуатационной документацией,
2. передал Пользователю (изготовленные в его присутствии) его закрытые ключи,
3. внес сертификаты открытых ключей Пользователя в реестр сертификатов,
4. зарегистрировал Пользователя в Системе,
5. передал Пользователю сертификаты открытых ключей Удостоверяющего центра,
6. провел обучение Пользователя правилам работы с СКЗИ,
7. список \_\_\_\_\_ отозванных \_\_\_\_\_ сертификатов (СОС) находится \_\_\_\_\_
8. \_\_\_\_\_ другие работы \_\_\_\_\_

Пользователь ознакомлен с Требованиями ФАПСИ по обеспечению безопасности информации при ее защите по уровню "С" (на уровне потребителя) и при работе с криптографическими ключами и СКЗИ будет выполнять эти требования.

**Пользователь**

\_\_\_\_\_ Фамилия И.О.

"\_\_\_"\_\_\_\_\_ 200\_г.

**Администратор  
Удостоверяющего центра**

\_\_\_\_\_ Фамилия И.О.

"\_\_\_"\_\_\_\_\_ 200\_г.

### **Требования ФАПСИ по обеспечению безопасности информации при ее защите по уровню “С” (на уровне потребителя)**

Защита информации по уровню “С” означает применение процедур электронной цифровой подписи и хеширования сертифицированных ФАПСИ средств криптографической информации, реализующих алгоритмы ГОСТ Р34.11-94, ГОСТ Р34.10-94 и ГОСТ 28147-89.

#### **1. Требования по организационному обеспечению эксплуатации СКЗИ**

1.1. На предприятии выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ.

1.2. На предприятии разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ.

1.3. К работе со СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.

#### **2. Требования по размещению СКЗИ и режиму охраны**

2.1. Помещения, в которых размещаются программно-технические средства со встроенными СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ.

2.2. Размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

2.3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

2.4. Входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.

2.5. Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

2.6. Размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна.

2.7. В режимные помещения допускаются Руководство Пользователя, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов.

2.8. Системные блоки ЭВМ со СКЗИ оборудуются средствами контроля вскрытия.

2.9. Ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ (возможно согласование с Удостоверяющим центром Сибири).

**3. Требования по обеспечению безопасности ключевой информации**

3.1. Носители секретных ключей ЭЦП, шифрования и инсталляционные дискеты с ПО СКЗИ на предприятии берутся на поэкземплярный учет в выделенных для этих целей журналах.

3.2. Учет и хранение секретных ключей поручается руководством предприятия специально выделенным сотрудникам.

3.3. Для хранения носителей секретных ключей ЭЦП и шифрования выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации.

3.4. Хранение ключей и инсталляционных дискет с ПО СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

3.5. Рабочие (актуальные) и резервные ключи хранятся отдельно, с обеспечением условия невозможности их одновременной компрометации.

3.6. При транспортировке носителей секретной ключевой информации обеспечиваются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

**Примечание:** требования по размещению СКЗИ определяются условиями лицензирования ФАПСИ, правилами эксплуатации сертифицированных СКЗИ и могут уточняться при подготовке Пользователя к включению в Систему.

## **ПОРЯДОК разрешения конфликтных ситуаций, возникающих в ходе осуществления электронного документооборота.**

### **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, пользователи "Удостоверяющего центра Сибири" исходят из того, что:

- в соответствии с действующим законодательством, документ в электронном виде, заверенный ЭЦП, является документом, имеющим юридическую силу, аналогичным бумажному, снабженному подписью и печатью;
- электронный документ порождает обязательства Пользователя перед другим Пользователем "Удостоверяющего центра Сибири", если документ оформлен надлежащим образом, заверен ЭЦП и доставлен другому Пользователем. При этом ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи, а сертификат ЭЦП отправителя действует.
- Подтверждением того, что электронный документ Пользователя принят пользователем-получателем, является получение Пользователем или надлежащим образом оформленной электронной квитанции о принятии его документа, или получение того же самого документа подписанного ЭЦП пользователя-получателя.
- Пользователь признает, что используемая в соответствии с настоящим Регламентом, система защиты информации, которая обеспечивает ЭЦП и шифрование, 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. Пользователь признает, что разбор конфликтной ситуации в отношении авторства, целостности и подлинности электронного документа заключается в доказательстве подписания конкретного электронного документа на конкретном ключе ЭЦП.

1.2. В соответствии с настоящим порядком подлежат разрешению конфликтные ситуации двух типов:

- некорректность входящего электронного документа или ЭЦП (конфликтная ситуация типа 1);
- для корректного электронного документа непризнание отправителем электронного документа факта отправки документа, а также его целостности и подлинности (конфликтная ситуация 2).

## **2. Порядок разрешения конфликтных ситуаций типа 1.**

Действия пользователей в данной ситуации заключаются в следующем.

Принимающая Сторона по телефону (или иным образом) запрашивает у отправляющей Стороны информацию о документе, подлинность которого вызывает сомнения. При получении подтверждения об отправке указанного документа, запрашивает повторное оформление и отправку данного документа.

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

A.1. Повторная проверка дала отрицательный результат. ЭЦП документа неверна.

В этом случае делается вывод о возможном нарушении действующего криптографического ключа, либо о неисправности программно-аппаратных средств одной из Сторон.

При этом необходимо:

- проверить сертификаты открытых ключей
- штатными средствами в соответствии с эксплуатационной документацией проверить целостность и неизменность программного обеспечения СКЗИ. И переустановить его в случае необходимости.

Если положительный результат не достигнут обратиться в "Удостоверяющий центр Сибири".

A.2. Повторная проверка дала положительный результат. ЭЦП документа верна.

## **3. Порядок разрешения конфликтных ситуаций типа 2.**

3.1. В случае, если один из Пользователей приходит к выводу, что другой пользователь ссылается на документ, исходящий от него, который им не отправлялся и/или его содержание изменено, этот Пользователь немедленно извещает "Удостоверяющий центр Сибири" о наличии конфликтной ситуации.

3.2. "Удостоверяющего центра Сибири" формирует Экспертную (согласительная) комиссию для разрешения конфликтной ситуации, в состав которой входят представители "Удостоверяющего центра Сибири" и Пользователи вовлеченные в конфликтную ситуацию. Дополнительно могут привлекаться авторитетные, независимые специалисты в области криптографической защиты информации.

3.3. В ходе работы Экспертной комиссии рассматриваются документы, в том числе электронные, относящиеся к предмету разногласий, и выполняется процедура проверки ЭЦП документа, являющегося предметом разбирательства, в соответствии с Инструкцией, приведенной в Приложении 7 к настоящему Регламенту. При этом могут быть использованы следующие эталонные данные:

- данные архива оригиналов принятых/отправленных документов;
- сертификаты ЭЦП с открытыми криптографическими ключами, выданные Удостоверяющим Центром;
- дистрибутивы СКЗИ;
- ключевые носители.

### **Инструкция по доказательству принадлежности ЭЦП при разборе конфликтных ситуаций**

Для проведения разбора конфликтной ситуации необходимы:

- Заверенный Удостоверяющим Центром (УЦ) сертификат открытого ключа ЭЦП Пользователя, подписавшего документ, подлинность или авторство которого оспаривается.

- Файл, содержащий текст документа и ЭЦП его автора, в отношении которого возникает конфликтная ситуация.

Для разбора конфликтной ситуации необходимо выполнить следующие действия:

- Произвести операцию проверки подписи электронного документа, авторство подписи которого оспаривается на рабочем месте Администратора УЦ.

- Распечатать протокол проверки подписи.

- Распечатать сертификат открытого ключа ЭЦП из базы данных (реестра) Удостоверяющего Центра.

- Сравнить сертификат открытого ключа ЭЦП представленного Стороной и распечатанный сертификат открытого ключа ЭЦП из базы данных Удостоверяющего Центра.

Авторство подписи под документом считается установленным, если совпадают открытые ключи ЭЦП представленного Стороной сертификата и сертификат открытого ключа ЭЦП из базы данных Удостоверяющего Центра, и в протоколе проверки подписи Пользователя сформирована запись “Подпись верна”.

**Акт  
Уничтожения криптографических ключей**

Настоящий акт составлен в том, что физически уничтожены ключевые носители (дискеты), содержащие криптографические ключи:

<b>№</b>	<b>Серийный номер ключа</b>	<b>Владелец ключа</b>
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____

Копии ключевых носителей в количестве \_\_\_\_\_ экз. уничтожены.

Сертификаты ключей переданы на архивное хранение

Владелец ключа \_\_\_\_\_ (Фамилия И.О.)

Руководитель Пользователя \_\_\_\_\_ (Фамилия И.О.)

М.П. « \_\_\_\_ » \_\_\_\_\_ 200\_ г.

Приказ

1. Создать при Центре технологий безопасности ТУСУР подразделение — Удостоверяющий Центр Сибири.
2. Считать Удостоверяющий центр Сибири представителем ТУСУР по использованию электронно-цифровой подписи и выполнению деятельности Удостоверяющего центра согласно ФЗ-1 от 10.01.2002 «Об электронной цифровой подписи»
3. Назначить руководителем Удостоверяющего центра Сибири д.т.н., профессора, руководителя ЦТБ ТУСУР Шелупанова А.А.
4. Назначить администратором Удостоверяющего центра Сибири к.ф-м.н., Филимонова Ю.М.
5. Шелупанову А.А., Мещерякову Р.В. и Филимонову Ю.М. в срок до 01.09.2004г. разработать регламент использования Удостоверяющего Центра Сибири в соответствии с действующим законодательством России.

Основание – представление руководителя ЦТБ ТУСУР Шелупанова А.А., официальное письмо ФАПСИ № ЛСЦ/Л-3831 от 24.06.2003г «Об использовании удостоверяющего центра»