Утверждено приказом
№ 8/01 от 16.09.2005

РЕГЛАМЕНТ

Удостоверяющего центра «Эксклюзивные решения»

Тольятти
2005

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ ... 3
1.1. Термины и определения ... 3
1.2. Область действия УЦ ... 4
1.3. Применение Регламента ... 5
1.4. Публикация Регламента ... 5
1.5. Порядок внесения изменений в Регламент ... 5
1.6. Контактная информация ... 5
2. УСЛУГИ УЦ ... 5
3. ОБЯЗАТЕЛЬСТВА СТОРОН ... 6
3.1. Обязательства УЦ ... 6
3.2. Обязательства Пользователя ... 6
4. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ... 6
4.1. Типы конфиденциальной информации ... 6
4.2. Типы информации, не являющейся конфиденциальной ... 6
4.3. Предоставление конфиденциальной информации ... 6
4.4. Защита конфиденциальной информации ... 7
5. ПЕРВОНАЧАЛЬНОЕ СОЗДАНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА ПОЛЬЗОВАТЕЛЯ ... 7
6. ПЕРЕДАЧА ПОЛЬЗОВАТЕЛЮ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА ... 7
7. ПЛАНОВАЯ СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА ... 8
8. ВНЕПЛАНОВАЯ СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА ... 8
9. АННУЛИРОВАНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА ... 8
10. ПРИОСТАНОВЛЕНИЕ ДЕЙСТВИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА ... 9
11. РАЗБОР КОНФЛИКТНЫХ СИТУАЦИЙ ... 9
12. СРОК И ПОРЯДОК ХРАНЕНИЯ СЕРТИФИКАТА В УЦ ... 9
13. ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ УЦ ... 9
14. ПРИЛОЖЕНИЯ К НАСТОЯЩЕМУ РЕГЛАМЕНТУ ... 9

1. ОБЩИЕ ПОЛОЖЕНИЯ

Компания «Эксклюзивные решения» действует как Удостоверяющий центр (УЦ) и осуществляет свою деятельность в соответствии с законодательством Российской Федерации и на основании лицензий ФСБ:

- на деятельность по техническому обслуживанию шифровальных (криптографических) средств №1259Х от 11.05.2004;
- на деятельность по распространению шифровальных (криптографических) средств №1260Р от 11.05.2004;
- на деятельность по предоставлению услуг в области шифрования информации №1261У от 11.05.2004.

Настоящий Регламент разработан на основании законов Российской Федерации от 20.02.1995 №24-ФЗ «Об информации, информатизации и защите информации», от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи», а также принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

Настоящий Регламент определяет область действия УЦ, его функции, правила и порядок работы всех вовлеченных сторон при взаимоотношениях, возникающих в процессе оказания услуг УЦ.

1.1. Термины и определения

Владелец корпоративной информационной системы (Владелец КИС) – юридическое лицо, осуществляющее владение и пользование корпоративной информационной системы.

Владелец сертификата открытого ключа электронной цифровой подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат открытого ключа электронной цифровой 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).

Владельцем сертификата открытого ключа электронной цифровой подписи может быть только физическое лицо (Пользователь).

Закрытый ключ - криптографический ключ, который хранится пользователем системы в тайне. Используется для формирования электронной цифровой подписи и/или шифрования данных.

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

Ключевая информация – совокупность криптографических ключей и сертификата открытого ключа электронной цифровой подписи.

Компрометация ключа - утрата доверия к тому, что используемые ключи недоступны посторонним лицам или подозрение, что ключи были временно доступны неуполномоченным лицам.

Корпоративная информационная система (КИС) - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Открытый ключ электронной цифровой подписи (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.

Плановая смена ключей - смена ключей с установленной в корпоративной информационной системе периодичностью, не вызванная компрометацией ключей.

Пользователь УЦ (Пользователь) - физическое лицо, зарегистрированное в Удостоверяющем центре и являющееся уполномоченным представителем Участника КИС (либо самостоятельно являющееся Участником КИС).

Реестр сертификатов – электронный документ, содержащий созданные УЦ Сертификаты, в форме электронных документов, с указанием даты и времени их выдачи, сведений о действии Сертификата (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи).

Сертификат открытого ключа электронной цифровой подписи (Сертификат, Сертификат ключа подписи) - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром Пользователю УЦ для подтверждения подлинности электронной цифровой подписи и идентификации Пользователя.

Список отозванных сертификатов (СОС) - созданный УЦ список сертификатов, отозванных (аннулированных) до окончания срока их действия.

Список Участников КИС – список Участников КИС, утвержденный Владельцем КИС.

Средства криптографической защиты информации (СКЗИ) – аппаратные и/или программные средства, обеспечивающие применение электронной цифровой подписи и шифрования.

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.

Удостоверяющий центр (УЦ) – ООО «Эксклюзивные решения», оказывающее услуги удостоверяющего центра в КИС в соответствии с законодательством РФ на основании договора с Владельцем КИС.

Участник КИС – любое физическое или юридическое лицо (в том числе Владелец КИС), пользующееся услугами корпоративной информационной системы и включенное в Список Участников КИС.

Электронный документ (ЭД) - документ, в котором информация представлена в электронной цифровой форме.

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.

1.2. Область действия УЦ

УЦ «Эксклюзивные решения» осуществляет свою деятельность в качестве удостоверяющего центра корпоративных информационных систем. УЦ обслуживает корпоративные информационные системы, использующие СКЗИ ViPNet, сертифицированное в соответствии с действующим законодательством РФ.

Пользователем УЦ может быть только физическое лицо, являющееся уполномоченным представителем Участника КИС (либо самостоятельно являющееся

Участником КИС). Условием предоставления услуг является заключение Договора на оказание услуг между УЦ и Участником КИС. Договор может быть заключен только с Участником КИС, включенным в Список Участников КИС, утвержденный Владельцем КИС.

1.3. Применение Регламента

Регламент налагает обязательства на все вовлеченные стороны на основании его добровольного признания взаимодействующими сторонами. Добровольное признание настоящего Регламента является обязательным условием при заключении Договора на оказание услуг.

Настоящий Регламент вступает в силу в отношении Участника КИС с момента заключения им с УЦ Договора об оказании услуг. Регламент действует в отношении Участника КИС в течение всего срока действия Договора с УЦ.

1.4. Публикация Регламента

Настоящий Регламент публикуется:

- в электронной форме - по адресу: http://it-exclusive.ru/ca;
- в бумажной форме по запросу через почтовый адрес: 445050, г.Тольятти, а/я 4683.

1.5. Порядок внесения изменений в Регламент

УЦ имеет право в одностороннем порядке менять положения настоящего Регламента.

Публикация новой редакции Регламента осуществляется способами, указанными в разделе 1.4 настоящего Регламента.

Стороны, принявшие Регламент (заключившие Договор на оказание услуг) до внесения в него изменений, письменно уведомляются Удостоверяющим центром о вступлении в силу новой редакции Регламента.

1.6. Контактная информация

Телефон: (8482) 26-4446

E-mail: ca@it-exclusive.ru

2. УСЛУГИ УЦ

В процессе своей деятельности УЦ предоставляет следующие виды услуг:

- создает криптографические ключи по обращению Пользователей с гарантией сохранения в тайне закрытых ключей;
- создает сертификаты открытых ключей электронной цифровой подписи;
- осуществляет приостановление и возобновление действия сертификатов, а также их отзыв (аннулирование);
- ведет Реестр изготовленных сертификатов;
- осуществляет проверку уникальности открытых ключей ЭЦП в Реестре сертификатов и архиве УЦ;
- осуществляет выдачу сертификатов в форме документов на бумажных носителях и/или в форме электронных документов с информацией об их действии;
- распространяет СКЗИ;
- выполняет мероприятия по техническому сопровождению СКЗИ;
- оказывает иные, связанные с использованием СКЗИ услуги.

3. ОБЯЗАТЕЛЬСТВА СТОРОН

3.1. Обязательства УЦ

- публиковать официальную редакцию Регламента и уведомлять Участников КИС о внесении в него изменений, в соответствии с пп.1.4 и 1.5 настоящего Регламента;
- обеспечивать работу собственных служб и сервисов в соответствии с настоящим Регламентом и законодательством Российской Федерации, регулирующим деятельность УЦ.

3.2. Обязательства Пользователя

- следовать положениям настоящего Регламента;
- эксплуатировать СКЗИ ViPNet в соответствии с условиями и требованиями эксплуатационной документации на СКЗИ;
- 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 криптографических ключей не уполномоченными на то лицами;
- предоставлять в полном объеме информацию, необходимую для оказания услуг;
- использовать только собственную уникальную ключевую информацию;
- не использовать для электронной цифровой подписи закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее другими лицами;
- хранить в тайне закрытые ключи, принимать все возможные меры для предотвращения их потери, раскрытия, модифицирования или несанкционированного использования;
- немедленно связаться с УЦ при наличии подозрений на компрометацию ключей.

4. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

4.1. Типы конфиденциальной информации

Закрытые ключи пользователя и пароль, предоставляемый Пользователю в процессе прохождения процедуры регистрации, являются конфиденциальной информацией.

Персональная и корпоративная информация Пользователей, содержащаяся в УЦ, не подлежащая непосредственной рассылке в качестве части Сертификата Пользователя, списка отозванных сертификатов, считается конфиденциальной и не публикуется.

4.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией является открытой информацией.

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

Информация, включаемая в Сертификаты Пользователей УЦ и списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной.

Также не считается конфиденциальной информация о настоящем Регламенте.

4.3. Предоставление конфиденциальной информации

Предоставление конфиденциальной информации третьим лицам допускается только в случаях, требующих раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.

Предоставление конфиденциальной информации третьим лицам в других случаях не допускается.

4.4. Защита конфиденциальной информации

УЦ обеспечивает защиту конфиденциальной информации в соответствии с законодательством Российской Федерации.

5. ПЕРВОНАЧАЛЬНОЕ СОЗДАНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА ПОЛЬЗОВАТЕЛЯ

Первоначальное создание криптографических ключей и Сертификата Пользователя осуществляется централизованно УЦ, с гарантией конфиденциальности закрытых ключей.

Владельцем криптографических ключей и Сертификата может быть только физическое лицо (Пользователь).

В тех случаях, когда Сертификат требуется для работы каких-либо программных приложений (автоматическая обработка информации), назначается ответственное лицо, на имя которого издается Сертификат.

Срок действия криптографических ключей и Сертификата Пользователя в КИС устанавливается Владельцем КИС, но не может превышать 12 месяцев. По истечении срока действия ключей и Сертификата необходимо произвести их замену в соответствии с разделом 7 настоящего Регламента.

Создание криптографических ключей и Сертификата осуществляется на основании «Заявки на создание сертификата ключа подписи» (Приложение №1). Заявка подписывается Пользователем собственноручно и подтверждается подписью руководителя и печатью Участника КИС. Содержащиеся в Заявке сведения подтверждаются приложением к Заявке копии паспорта, заверенной подписью руководителя и печатью Участника КИС.

Сертификат создается:

- в форме электронного документа, заверенного ЭЦП уполномоченного лица УЦ;
- в форме документа на бумажном носителе, на бланке УЦ, заверенного собственноручной подписью уполномоченного лица и печатью УЦ.

Созданные криптографические ключи и Сертификат Пользователя, в форме электронного документа записываются на ключевой носитель. Передача ключевого носителя и Сертификата Пользователя в форме документа на бумажном носителе осуществляется в соответствии с разделом 6 настоящего Регламента.

При создании сертификатов, УЦ проверяет уникальность имени Пользователя и открытых ключей в Реестре и архиве УЦ.

6. ПЕРЕДАЧА ПОЛЬЗОВАТЕЛЮ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА

Передача криптографических ключей и Сертификата Пользователя осуществляется:

- из рук в руки по личному прибытию Пользователя в офис УЦ;
- отправкой специальной фельдъегерской связью (ФГУП «Главный центр специальной связи», http://www.cccb.ru) по адресу, указанному Пользователем в «Заявке на создание сертификата ключа подписи» (Приложение №1).

Способ выдачи ключей и Сертификата указывается в «Заявке на создание сертификата ключа подписи» (Приложение №1).

7. ПЛАНОВАЯ СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА

Плановая смена ключей и Сертификата производится Пользователем не позднее 15 дней до истечения срока действия Сертификата. Оповещение Пользователя о необходимости смены ключей производится автоматически СКЗИ ViPNet.

Для плановой смены криптографических ключей и Сертификата Пользователю необходимо:

1. Создать новые криптографические ключи.
2. С помощью СКЗИ ViPNet оформить и передать в УЦ запрос на Сертификат.
3. Оформить «Заявку на создание сертификата ключа подписи» (Приложение №1).
4. После создания Сертификата Удостоверяющим центром, получить созданный Сертификат и ввести его в действие, в соответствии с эксплуатационной и технической документацией на СКЗИ ViPNet.

8. ВНЕПЛАНОВАЯ СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА

Внеплановая смена криптографических ключей и Сертификата Пользователя производится по следующим причинам:

- компрометация или подозрение на компрометацию криптографических ключей и Сертификата;
- изменение идентифицирующей информации или атрибутов Пользователя в Сертификате до истечения срока действия Сертификата;

К событиям, связанным с компрометацией криптографических ключей относятся следующие события:

- утрата ключевых носителей криптографических ключей;
- утрата ключевых носителей с последующим обнаружением;
- утрата ключей от сейфа, хранилища в момент нахождения в нем ключевых носителей криптографических ключей;
- иные обстоятельства прямо или косвенно свидетельствующие о наличии возможности доступа к криптографическим ключам третьих или неуполномоченных лиц.

При возникновении указанных выше причин Участнику КИС необходимо подать в УЦ «Заявку на аннулирование сертификата ключа подписи» (Приложение №2), на основании которой УЦ аннулирует текущие криптографические ключи и Сертификат Пользователя.

Изготовление новых ключей и сертификата происходит в соответствии с разделом 7 настоящего Регламента.

9. АННУЛИРОВАНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА

Аннулирование Сертификата Пользователя производится по следующим причинам:

- по истечении срока его действия;
- в случае прекращения действия Договора на оказание услуг;
- в случае отстранения Пользователя от выполнения служебных обязанностей;
- в случае увольнения Пользователя;
- в случаях, указанных в разделе 8 настоящего Регламента.

При возникновении указанных выше причин (за исключением пп. 1 и 2) Участнику КИС необходимо подать в УЦ «Заявку на аннулирование сертификата ключа подписи» (Приложение №2), на основании которой УЦ аннулирует текущие криптографические ключи и Сертификат Пользователя.

В случае аннулирования Сертификата Пользователя, информация о нем помещается в СОС, который публикуется при помощи соответствующей функции СКЗИ ViPNet.

10. ПРИОСТАНОВЛЕНИЕ ДЕЙСТВИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА

Приостановление действия Сертификата Пользователя производится в случаях:

- невыполнения Пользователем или Участником КИС положений настоящего Регламента и/или Договора на оказание услуг;
- по решению Владельца КИС.

Период времени, на который УЦ приостанавливает действие Сертификата Пользователя определяется в каждом конкретном случае индивидуально, до момента разрешения всех разногласий.

УЦ оповещает о факте приостановления действия Сертификата Пользователя следующие стороны:

- Пользователя, сертификат которого был приостановлен, с указанием причины приостановления сертификата;
- Владельца КИС;
- остальных Пользователей, путем внесения в Реестр сертификатов информации о приостановлении действия Сертификата Пользователя, который публикуется при помощи соответствующей функции СКЗИ ViPNet.

11. РАЗБОР КОНФЛИКТНЫХ СИТУАЦИЙ

Разбор конфликтных ситуаций происходит в соответствии с «Порядком разрешения конфликтных ситуаций» (Приложение №3), входящим в комплект эксплуатационной и технической документации на СКЗИ ViPNet.

12. СРОК И ПОРЯДОК ХРАНЕНИЯ СЕРТИФИКАТА В УЦ

Хранение Сертификата Пользователя в форме электронного документа осуществляется в Реестре сертификатов в течение срока действия Сертификата.

По истечении срока действия Сертификат в форме электронного документа исключается из Реестра сертификатов и переводится в режим архивного хранения. Срок архивного хранения составляет 5 лет.

Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

13. ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ УЦ

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

В случае прекращения деятельности УЦ, Реестр изготовленных Сертификатов передается в архив уполномоченного федерального органа исполнительной власти, а также владельцу соответствующей корпоративной информационной системы.

14. ПРИЛОЖЕНИЯ К НАСТОЯЩЕМУ РЕГЛАМЕНТУ

Приложение №1 Заявка на создание сертификата ключа подписи

Приложение №2 Заявка на аннулирование сертификата ключа подписи

Приложение №3 Порядок разрешения конфликтных ситуаций