

**Общество с ограниченной ответственностью
“Украинский сертификационный центр”**

СОГЛАСОВАНО

Начальник ДСТСЗИ
СБ Украины

_____ К.Бойко

“ ___ ” _____ 2006 р.

УТВЕРЖДАЮ

Директор ООО “Украинский
сертификационный центр”

_____ А. Шаталов

“ ___ ” _____ 2006 р.

УКРАИНСКИЙ СЕРТИФИКАЦИОННЫЙ ЦЕНТР

Шифр (“Сертификат”)

РЕГЛАМЕНТ РАБОТЫ ЦЕНТРА СЕРТИФИКАЦИИ КЛЮЧЕЙ

804. 33406510.466451.001.РГ.01

На 32 листах

1	Введение	7
1.1	Обзор.....	8
1.1.1	Роль Регламента УСЦ и Договоров	8
1.1.2	Основные требования.....	8
1.1.3	Нормативные документы	8
1.2	Идентификация	9
1.3	Система «Сертификат»	9
1.3.1	Сертификационный центр	9
1.3.2	Регистрационные центры.....	9
1.3.3	Клиенты и Пользователи УСЦ.....	10
1.3.4	Применение заявок	10
1.3.4.1	Заявки на сертификат общего назначения	10
1.3.4.2	Ограничения использования сертификата	10
1.3.4.3	Запрещенное использование сертификата	10
1.4	Сведения о контактах	10
1.4.1	Организация, формирующая Регламент.....	10
1.4.2	Адрес Украинского сертификационного центра	10
2	Основные определения	11
2.1	Обязательства.....	11
2.1.1	Обязательства Украинского сертификационного центра.....	11
2.1.2	Обязательства Регистрационного центра.....	11
2.1.3	Обязательства Клиента	11
2.1.4	Обязательства уполномоченного лица	11
2.1.5	Обязательства отдела архива данных УСЦ.....	11
2.2	Ответственность	11
2.2.1	Ответственность УСЦ	11
2.2.1.1	Гарантии УСЦ Пользователю или Уполномоченному лицу.....	11
2.2.1.2	Отказы от гарантий УСЦ	11
2.2.1.3	Ограничения ответственности УСЦ	11
2.2.1.4	Форс-мажорные обстоятельства	11
2.2.2	Ответственность Регистрационного центра.....	12
2.2.3	Ответственность Пользователя	12
2.2.3.1	Гарантии Пользователя	12
2.2.3.2	Компрометация секретного ключа.....	12
2.2.4	Ответственность уполномоченного лица.....	12
2.3	Финансовая ответственность.....	12
2.3.1	Компенсации Пользователей и уполномоченных лиц.....	12
2.3.1.1	Компенсации УСЦ от Пользователей.....	12
2.3.1.2	Компенсация УСЦ от Доверенных лиц.....	12
2.3.2	Имущественные отношения доверительного характера.....	12
2.3.3	Административные процессы	12
2.4	Пояснение и взыскание	12
2.4.1	Законы государства	12
2.4.2	Обязательство и ответственность в договоре, страхование, предмет договора, уведомление сторон.....	12
2.4.3	Процедуры решения споров	12
2.4.3.1	Споры между УСЦ и Пользователем	12
2.4.3.2	Споры между УСЦ и РЦ.....	12
2.5	Условия оплаты	13
2.5.1	Оплата за выдачу сертификата или его обновление	13
2.5.2	Оплата при запросе на доступ к сертификату	13

2.5.3	Оплата за отзыв сертификата или за предоставление информации о статусе сертификата.....	13
2.5.4	Оплата за другие услуги типа информации политики безопасности сертификата.....	13
2.5.5	Политика возврата платежей за сертификат.....	13
2.5.5.1	До создания сертификата.....	13
2.5.5.2	После создания сертификата.....	13
2.5.6	Переиздание сертификата.....	13
2.6	Предоставление информации УСЦ и обслуживание базы данных сертификатов.....	13
2.6.1	Предоставление информации УСЦ.....	13
2.6.2	Периодичность предоставления информации.....	13
2.6.3	Контроль доступа на предоставление информации УСЦ.....	14
2.6.4	База данных УСЦ.....	14
2.7	Проверка работоспособности УСЦ.....	14
2.7.1	Частота проверки работоспособности УСЦ.....	14
2.7.2	Идентификация и уровень квалификации проверяющей организации.....	14
2.7.3	Взаимоотношения проверяющей организации с Клиентом.....	14
2.7.4	Список разделов, не подлежащих проверке.....	14
2.7.5	Меры при выявлении ошибок методики проверки работоспособности.....	14
2.7.6	Предоставление результатов проверки.....	14
2.8	Конфиденциальность и секретность.....	14
2.8.1	Типы информации, которые являются конфиденциальной.....	14
2.8.2	Типы информации, которые не конфиденциальны.....	15
2.8.3	Предоставление информации об отозванных или заблокированных сертификатах.....	15
2.8.4	Официальное требование выдачи информации конфиденциального характера по закону	15
2.8.5	Обстоятельства, при которых предоставляются документы.....	15
2.8.6	Раскрытие информации по требованию Клиента.....	15
2.8.7	Обстоятельства, при которых предоставляется информация.....	15
2.9	Права на интеллектуальную собственность.....	15
2.9.1	Права на сертификаты и информацию о списках отозванных сертификатов.....	15
2.9.2	Права на спецификацию политики безопасности сертификатов.....	15
2.9.3	Права на имена.....	16
2.9.4	Права на ключи и на данные о ключах.....	16
3	Идентификация и аутентификация.....	16
3.1	Начальная регистрация.....	16
3.1.1	Типы имен.....	16
3.1.1.1	Сертификаты УСЦ.....	16
3.1.1.2	Клиентские сертификаты УСЦ.....	16
3.1.2	Понятность имен.....	16
3.1.3	Правила интерпретации разных форм имен.....	16
3.1.4	Уникальность имени.....	16
3.1.5	Разрешение споров, связанных с использованием имен.....	16
3.1.6	Процедура распознавания, аутентификации и роль торговой марки.....	16
3.1.7	Проверка факта обладания секретным ключом.....	17
3.1.8	Аутентификация подлинности организации.....	17
3.1.8.1	Аутентификация подлинности организации Клиента.....	17
3.1.8.2	Аутентификация подлинности УСЦ.....	17
3.1.9	Аутентификация персональных данных Клиента.....	17
3.2	Порядок повторной выдачи ключей или обновления сертификата.....	17
3.3	Повторная выдача ключей после отзыва сертификата.....	17
3.4	Заявка на отзыв сертификат.....	17
4	Порядок издания сертификатов.....	18

4.1	Создание заявки на сертификат	18
4.2	Создание сертификата Клиента.....	18
4.3	Принятие сертификата	18
4.4	Блокирование и отзыв сертификата.....	18
4.4.1	Обстоятельства для отзыва сертификата.....	18
4.4.1.1	Обстоятельства для отзыва сертификата Клиента	18
4.4.1.2	Обстоятельства для отзыва сертификата УСЦ.....	19
4.4.2	Кто может отозвать сертификат	19
4.4.2.1	Кто может отозвать сертификат Клиента.....	19
4.4.2.2	Кто может отозвать сертификат УСЦ	19
4.4.3	Процедуры отзыва сертификата Клиента	19
4.4.3.1	Процедура отзыва сертификата Клиента	19
4.4.3.2	Процедура отзыва сертификата УСЦ	19
4.4.4	Период отсрочки отзыва сертификата.....	19
4.4.5	Обстоятельства, при которых сертификат может быть заблокирован.....	19
4.4.6	Кто может заблокировать сертификат.....	20
4.4.7	Процедуры, используемые для блокирования сертификата	20
4.4.8	Ограничения для периода блокирования сертификата.....	20
4.4.9	Частота формирования списка отозванных сертификатов.....	20
4.4.10	Правила использования списка отозванных сертификатов Клиентами УСЦ	20
4.4.11	Возможность получения информации о статусе сертификата в реальном времени ..	20
4.4.12	Правила использования клиентом информации о состоянии сертификата в режиме реального времени	20
4.4.13	Наличие дополнительных способов оповещения об отзыве сертификатов	20
4.4.14	Правила использования Пользователями дополнительных способов оповещения об отзыве сертификатов	20
4.4.15	Особые требования к действиям УСЦ при компрометации секретного ключа УСЦ.....	20
4.5	Процедуры контроля защиты	20
4.5.1	Виды записанных событий	20
4.5.2	Периодичность процесса записи события.....	21
4.5.3	Срок хранения журналов	21
4.5.4	Защита журналов	21
4.5.5	Резервное копирование журнала.....	21
4.5.6	Тип системы ведения журналов аудита (встроенная/внешняя).....	21
4.5.7	Система оповещения Клиентов о компрометации секретного ключа	21
4.5.8	Анализ безопасности УСЦ.....	21
4.6	Архивация.....	22
4.6.1	Виды записанных событий	22
4.6.2	Срок хранения архива	22
4.6.3	Защита архива	22
4.6.4	Процедура создания резервной копии архива	22
4.6.5	Требования фиксации времени создания записей в архиве	22
4.6.6	Описание системы архивации (встроенная/внешняя, доступ и т.д.).....	22
4.7	Плановая замена ключей.....	22
4.8	Действия в аварийной ситуации или при компрометации ключа УСЦ.....	22
4.8.1	Порча оборудования, программного обеспечения или искажение данных.....	22
4.8.2	Восстановление работоспособности УСЦ в случае аварии	23
4.8.3	Восстановление работоспособности УСЦ в случае компрометация ключа.....	23
4.9	Прекращение деятельности УСЦ.....	23
5	Контроль защиты оборудования УСЦ, процесса работы этого оборудования и персонала.....	23
5.1	Физический контроль	23
5.1.1	Конструкция и размещение рабочих мест	23

5.1.2	Физический доступ	23
5.1.3	Кондиционирование воздуха и электрическое питание	24
5.1.4	Уровень влажности.....	24
5.1.5	Обеспечение противопожарной защиты	24
5.1.6	Уровень шума	24
5.1.7	Утилизация отходов	24
5.1.8	Сохранение архивов вне УСЦ	24
5.2	Процедурный контроль	24
5.2.1	Доверенные роли	24
5.2.2	Требуемое количество людей для выполнения определенного задания	25
5.2.3	Идентификация и аутентификация человека для каждой роли	25
5.3	Требования к персоналу УСЦ	26
5.3.1	Требования по знаниям, уровню квалификации, опыту и категории допуска.....	26
5.3.2	Основы процедуры проверки	26
5.3.3	Требования по обучению персонала.....	26
5.3.4	Частота переобучения и требования по переобучению.....	26
5.3.5	График работы	26
5.3.6	Санкции за неправомерные действия.....	26
5.3.7	Требования по заключению контракта с персоналом.....	26
5.3.8	Доступ к документации УСЦ	26
6	Технический контроль защиты	26
6.1	Установка программного обеспечения и генерация пары ключей.....	26
6.1.1	Генерация пары ключей.....	26
6.1.2	Доставка секретного ключа Клиенту.....	26
6.1.3	Доставка открытого ключа Издателю сертификата	27
6.1.4	Доставка открытого ключа Клиенту.....	27
6.1.5	Размеры ключа	27
6.1.6	Параметры генерации открытого ключа	27
6.1.7	Проверка качества параметров генерации ключей	27
6.1.8	Программное обеспечение для генерации пары ключей.....	27
6.1.9	Назначение ключа.....	27
6.2	Защита секретного ключа	27
6.2.1	Стандарты для криптографических модулей.....	27
6.2.2	Доступ к секретному ключу УСЦ.....	28
6.2.3	Возможность предоставления доступа к секретному ключу посторонним организациям.....	28
6.2.4	Создание копий секретного ключа	28
6.2.5	Архивирование секретного ключа	28
6.2.6	Введение секретного ключа в криптографический модуль	28
6.2.7	Метод активации секретного ключа	28
6.2.7.1	Секретный ключ Клиента	28
6.2.7.1.1	Сертификат с обычным уровнем защиты.....	28
6.2.7.1.2	Сертификат с повышенным уровнем защиты.....	29
6.2.7.2	Секретный ключ УСЦ	29
6.2.8	Метод блокирования секретного ключа.....	29
6.2.9	Метод ликвидации секретного ключа	29
6.3	Другие аспекты управления парой ключей.....	29
6.3.1	Секретный архивный ключ.....	29
6.3.2	Период использования открытого и секретного ключа.....	29
6.4	Данные для начала срока действия секретного ключа	29
6.4.1	Установка и создание данных для секретного ключа.....	29
6.4.2	Защита данных секретного ключа	30

6.4.3	Другие аспекты для данных секретного ключа	30
6.5	Контроль компьютерной защиты.....	30
6.5.1	Специфика технических требований компьютерной защиты.....	30
6.5.2	Уровень компьютерной защиты.....	30
6.6	Технический контроль жизненного цикла	30
6.6.1	Контроль развития системы	30
6.6.2	Контроль управления системой защиты	30
6.7	Контроль сетевой системы защиты	30
6.8	Контроль построения криптографического модуля.....	30
7	Профили сертификата открытых ключей и списка отозванных сертификатов	30
8	Руководство по регламенту	31
8.1	Процедура внесения изменений в Регламент	31
8.1.1	Пункты, которые можно изменять без уведомления	31
8.1.2	Пункты, которые можно изменять с уведомлением	31
8.1.2.1	Перечень пунктов, который можно изменять, но с уведомлением	31
8.1.2.2	Механизм уведомления.....	31
8.1.2.3	Период комментария изменений.....	31
8.1.2.4	Механизм трактовки комментария изменений.....	31
8.2	Публикации и уведомления УСЦ	31
8.3	Процедура утверждения Регламента	31
9	Условные обозначения и определения	31
9.1	Перечень условных обозначений.....	31
9.2	Определения.....	32

1 ВВЕДЕНИЕ

Данный документ определяет основные правила работы Украинского сертификационного центра (далее – УСЦ). Регламент является общедоступным документом. Детальное описание всех аспектов функционирования Украинского сертификационного центра содержится во внутренних документах центра, которые не подлежат публикации и предоставляются уполномоченным организациям в случаях, определенных законодательством Украины.

Международные стандарты ISO/IEC, IETF, ETSI определяют и стандартизируют широкий круг решений в сфере использования технологии инфраструктуры открытых ключей (Public key infrastructure). Для обеспечения совместимости программного обеспечения, упомянутые стандарты предусматривают гибкость относительно технических аспектов: протоколов, форматов данных, технологических процедур. Для некоторых параметров объектов они предусматривают перечень альтернативных реализаций. В то же время некоторые специфические аспекты не охватываются, не учитываются и требования украинского законодательства. С целью обеспечения совместимости программно-технических решений, которые используются в Украинском сертификационном центре и у Пользователя, разработаны технические спецификации, основанные на международных стандартах. Эти документы предназначены для:

- определения ряда стандартов, которых необходимо придерживаться в программном обеспечении Украинского сертификационного центра и Пользователя;
- ограничения возможных альтернативных реализаций, которые предусматривают международные стандарты;
- установки технических требований к объектам, которые не охватываются международными стандартами, но вместе с тем нужны для обеспечения совместимости.

1.1 Обзор

1.1.1 Роль Регламента УСЦ и Договоров

Регламент УСЦ определяет работу УСЦ, юридическую и техническую инфраструктуру, а именно:

- Обязанности УСЦ, Регистрационного центра, Пользователей и Уполномоченных лиц;
- Правовые вопросы, согласно договору УСЦ с Пользователем, УСЦ с Уполномоченным лицом;
- Предназначение системы «Сертификат»;
- Применяемые стандарты, алгоритмы, подтверждение данных сертификата Клиента;
- Процедуры по обслуживанию сертификата, заявки на сертификат, отзыв и блокирование сертификата;
- Процедуры по учету и хранению базы данных сертификатов;
- Управление сертификатами открытых ключей;
- Формирование списков отозванных сертификатов;

1.1.2 Основные требования

В соответствии с Законом Украины «Об электронной цифровой подписи» УСЦ должен использовать надежные средства электронной цифровой подписи.

Средства электронной цифровой подписи должны иметь сертификат соответствия или положительный экспертный вывод по результатам государственной экспертизы в сфере криптографической защиты информации. Электронная цифровая подпись должна быть реализована на основе национальных криптографических алгоритмов и стандартов. Допускается использование криптографических алгоритмов, определенных международными стандартами.

Для обеспечения представления в усиленном сертификате криптографических алгоритмов и их параметров, которые являются государственными стандартами, используется дерево объектных идентификаторов, определенное в соответствии с «Правилами усиленной сертификации», утвержденных приказом Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины № 3 от 13.01.2005. Для представления в сертификате криптографических алгоритмов и их параметров, которые не охвачены этим документом, используются собственные объектные идентификаторы. Вместе с тем, объектные идентификаторы для национальных криптографических алгоритмов не зарегистрированы, как это предусмотрено международными стандартами, и используются только для обеспечения совместимости в рамках УСЦ. Для иностранных криптографических алгоритмов используются зарегистрированные объектные идентификаторы.

1.1.3 Нормативные документы

- Закон Украины «Об электронной цифровой подписи»,
- постановления Кабинета Министров Украины:
 - от 26.05.04 № 680 «Об утверждении Порядка удостоверения наличия электронного документа (электронных данных) на определенный момент времени»;
 - от 13.07.04 № 903 «Об утверждении Порядка аккредитации центра сертификации ключей»;
 - от 28.10.04 № 1451 «Об утверждении Положения о центральном удостоверяющем органе»;
 - от 28.10.04 № 1452 «Об утверждении Порядка применения электронной цифровой подписи органами государственной власти, органами местного самоуправления, предприятиями, учреждениями и организациями государственной формы собственности»;
 - от 28.10.04 № 1454 «Об утверждении Порядка обязательной передачи документированной информации»;

- «Правила усиленной сертификации», утвержденные приказом Департамента специальных телекоммуникационных систем и защиты информации Службы безопасности Украины № 3 от 13.01.2005;

1.2 Идентификация

Документ является Регламентом Украинского сертификационного центра, реквизиты которого представлены в п.1.4.2.

1.3 Система «Сертификат»

Назначения системы: управление сертификатами открытых ключей асимметрических криптографических преобразований.

1.3.1 Сертификационный центр

Украинский сертификационный центр (УСЦ) используется для:

- создания структуры базы данных и управления массивами информации;
- вычисления параметров необходимых для криптографических преобразований, которые используются в самом центре;
- создания пары секретных и открытых ключей, вычисления сертификатов открытых ключей (корневых, корпоративных, операторских) Украинского сертификационного центра, которые отвечают требованиям Правил усиленной сертификации;
- создания сертификатов открытых ключей по заявкам, которые содержат открытые ключи, а также усиленных сертификатов, которые отвечают требованиям Правил усиленной сертификации;
- управления сертификатами открытых ключей (введение в базу данных, выборка из базы данных, проверка целостности, экспорт в бинарном формате и формате base64, импорт в бинарном формате и формате base64, отзыв сертификатов);
- создания списков отозванных сертификатов открытых ключей в формате X.509 версии 2;
- управления списками отозванных сертификатов открытых ключей (внесения сертификата в список, экспорт в бинарном формате, импорт в бинарном формате, проверка целостности списка, создания частичных списков отозванных сертификатов);
- отзыва сертификатов открытых ключей по заявкам или по собственной инициативе;
- управления доступом Пользователей к сертификатам открытых ключей и персонала УСЦ к базе данных;
- ведения протоколов работы УСЦ;
- обеспечения синхронизации с Всемирным координированным временем (UTC) с точностью до одной секунды;
- использования времени в отметке времени по киевскому времени;
- формирования по заявке Пользователя криптографической отметки времени;
- формирования по заявке Пользователя данных о текущем состоянии сертификата открытого ключа;

Программно-технический комплекс УСЦ представляет собой программно-аппаратный комплекс по созданию, хранению, управлению и распределению сертификатов открытых ключей.

1.3.2 Регистрационные центры

Регистрационный центр является подразделением УСЦ. Регистрационный центр УСЦ используется для:

- создания структуры базы данных и управления массивами информации;
- вычисления параметров, необходимых для криптографических преобразований, которые используются в самом регистрационном центре;
- создания собственной пары ключей, получения сертификата Регистрационного центра от УСЦ;

- формирование подписанной секретным ключом ЭЦП Регистрационного центра заявки в УСЦ на формирование сертификата ключа электронной цифровой подписи Клиента;
- транспортировки заявки Клиента в УСЦ, получения сертификата ключа ЭЦП Клиента от УСЦ;
- обеспечения обмена данными с УСЦ в защищенном виде.

1.3.3 Клиенты и Пользователи УСЦ

Любое физическое или юридическое лицо может получить сертификат открытого ключа. Для этого необходимо создать пару ключей и сформировать заявку на получение сертификата открытого ключа. Заявку и документы, удостоверяющие лицо, необходимо доставить в УСЦ или Регистрационный центр УСЦ. После получения сертификата ключа ЭЦП указанное лицо становится клиентом УСЦ. Любое физическое или юридическое лицо может постоянно получать информацию о статусе сертификата открытого ключа Клиента. Указанное лицо становится пользователем УСЦ.

1.3.4 Применение заявок

Заявки предназначены для создания сертификатов Клиента и внесения их в базу данных УСЦ. Заявки содержат открытый ключ и набор идентификационных данных Клиента. УСЦ формирует сертификат открытого ключа с набором данных в соответствии с договором УСЦ с Клиентом.

1.3.4.1 Заявки на сертификат общего назначения

Клиент УСЦ доверяет уполномоченному лицу подписывать его заявку на сертификат ЭЦП. Согласно закону Украины «Об электронной цифровой подписи» УСЦ подтверждает, что данные, подписанные электронной цифровой подписью, которую можно проверить с помощью сертификата, действительны, но ограничиваются сроком действия самого сертификата.

1.3.4.2 Ограничения использования сертификата

Сертификаты УСЦ предназначены для общего применения. Сертификаты могут иметь ограничения в использовании. Данные об ограничении использования сертификата включаются в сертификат.

Сертификат Клиента не может использоваться, как сертификат УСЦ. Это ограничение подтверждается отсутствием расширения основных ограничений. См. п.7.1.2

Сертификаты могут использоваться только в соответствии с их предназначением.

1.3.4.3 Запрещенное использование сертификата

Сертификаты УСЦ не предназначены для редактирования, изменения, перепродажи или использованию не по назначению. Запрещено использование сертификата при операциях, связанных с риском остановки оборудования, ущерба, смерти. Сертификаты с низким уровнем политики безопасности не должны использоваться как средство идентификации личности.

1.4 Сведения о контактах

1.4.1 Организация, формирующая Регламент

Адрес организации, формирующей Регламент:
ТОВ „Украинский сертификационный центр”
04119, м. Киев, ул. Дегтяревская, 36, оф.617;
т. (044) 496-25-21, т. (044) 496-25-22;
e-mail: info@ukrcc.com

1.4.2 Адрес Украинского сертификационного центра

ООО „Украинский сертификационный центр”
04119, м. Киев, ул. Дегтяревская, 36, оф. 617;

т.ф. (044) 496-25-21, т. (044) 496-25-22
Веб-сайт УСЦ: <http://www.ukrcc.com>
Подача заявок по e-mail: info@ukrcc.com
Служба отметок времени (Timestamp): 83.170.246.26:139
Служба состояния сертификата (OCSP): 83.170.246.26:2560

2 ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

2.1 Обязательства

2.1.1 Обязательства Украинского сертификационного центра

Обязательства Украинского сертификационного центра определяются данным регламентом и договорами Украинского сертификационного центра с другими лицами.

2.1.2 Обязательства Регистрационного центра

Обязательства Регистрационного центра определяются данным регламентом.

2.1.3 Обязательства Клиента

Обязательства Клиента определяются его договором с Украинским сертификационным центром.

2.1.4 Обязательства уполномоченного лица

Обязательства уполномоченного лица определяются договором уполномоченного лица с Украинским сертификационным центром. Обязанности уполномоченного лица определяются в соответствии с договором между Клиентом и уполномоченным лицом.

2.1.5 Обязательства отдела архива данных УСЦ

Обязательства отдела архива данных определяются данным регламентом.

2.2 Ответственность

2.2.1 Ответственность УСЦ

Ответственность УСЦ о выполнении обязательств согласно договору Украинского сертификационного центра с другими лицами.

2.2.1.1 Гарантии УСЦ Пользователю или Уполномоченному лицу

Гарантии УСЦ по обеспечению качества предоставляемых УСЦ услуг ЭЦП Пользователю или уполномоченному лицу предоставляются согласно договору с УСЦ.

2.2.1.2 Отказы от гарантий УСЦ

Отказы от вышеперечисленных гарантий УСЦ согласно договору Украинского сертификационного центра с другими лицами.

2.2.1.3 Ограничения ответственности УСЦ

Ограничения ответственности УСЦ согласно договору Украинского сертификационного центра с другими лицами.

2.2.1.4 Форс-мажорные обстоятельства

Форс-мажорные обстоятельства согласно договору Украинского сертификационного центра с другими лицами.

2.2.2 Ответственность Регистрационного центра

Поскольку Регистрационный центр является подразделением УСЦ, то ответственность РЦ не предусматривается.

2.2.3 Ответственность Пользователя

Согласно договору с Украинским сертификационным центром.

2.2.3.1 Гарантии Пользователя

Согласно договору с Украинским сертификационным центром.

2.2.3.2 Компрометация секретного ключа

Регламент устанавливает требования для защиты секретного ключа Клиента, которые приведены в Регламенте УСЦ, п 6.2.7.1 и в договоре Клиента с УСЦ. В договоре указывается, что Клиент несет ответственность за потерю, компрометацию или изменение данных секретного ключа.

2.2.4 Ответственность уполномоченного лица

Согласно договору с Украинским сертификационным центром.

2.3 Финансовая ответственность

Согласно договору Украинского сертификационного центра с другими лицами.

2.3.1 Компенсации Пользователей и уполномоченных лиц

2.3.1.1 Компенсации УСЦ от Пользователей

Согласно договору Украинского сертификационного центра с Пользователем.

2.3.1.2 Компенсация УСЦ от Доверенных лиц

Согласно договору Украинского сертификационного центра с уполномоченным лицом.

2.3.2 Имущественные отношения доверительного характера

Согласно договору Украинского сертификационного центра с другими лицами.

2.3.3 Административные процессы

Украинский сертификационный центр и его Регистрационные центры застрахованы.

2.4 Пояснение и взыскание

2.4.1 Законы государства

Услуги, которые предоставляются Украинским сертификационным центром, соответствуют Закону Украины “Об электронной цифровой подписи”.

2.4.2 Обязательство и ответственность в договоре, страхование, предмет договора, уведомление сторон

Согласно договору с Украинским сертификационным центром.

2.4.3 Процедуры решения споров

2.4.3.1 Споры между УСЦ и Пользователем

Споры между УСЦ и Пользователем происходят в порядке, установленном законодательством Украины.

2.4.3.2 Споры между УСЦ и РЦ

Не предусматривается

2.5 Условия оплаты

2.5.1 Оплата за выдачу сертификата или его обновление

Согласно договору с Украинским сертификационным центром.

2.5.2 Оплата при запросе на доступ к сертификату

Сертификат доступен при условии согласия Клиента на его распространение. Оплата при запросе на доступ к сертификату не предусмотрена.

2.5.3 Оплата за отзыв сертификата или за предоставление информации о статусе сертификата

Согласно договору с Украинским сертификационным центром.

Оплата за отзыв сертификата или за предоставление информации о статусе сертификата не предусмотрена.

2.5.4 Оплата за другие услуги типа информации политики безопасности сертификата

Согласно договору с Украинским сертификационным центром.

2.5.5 Политика возврата платежей за сертификат

2.5.5.1 До создания сертификата

Согласно договору с Украинским сертификационным центром.

2.5.5.2 После создания сертификата

Согласно договору с Украинским сертификационным центром.

2.5.6 Переиздание сертификата

Согласно определенной и установленной политике и практике, УСЦ не переиздает сертификат Клиента с использованием ранее сформированных ключей ЕЦП.

2.6 Предоставление информации УСЦ и обслуживание базы данных сертификатов

2.6.1 Предоставление информации УСЦ

УСЦ обслуживает базу данных сертификатов. УСЦ предоставляет Регламент, формы договора с Пользователем (или Клиентом) и договора с уполномоченным лицом на Веб-сайте УСЦ, в разделе «Сертификационный центр – Регламент работы» по адресу: <http://83.170.246.26>. УСЦ предоставляет сертификаты в соответствии с таблицей 2.6

Таблица 2.6

Тип сертификата	Использование
Корневой сертификат УСЦ	Сертификат используется для создания Корпоративного сертификата, а также для его проверки в цепочке сертификатов.
Корпоративный сертификат УСЦ	Сертификат используется для создания клиентского сертификата, а также для его проверки в цепочке сертификатов.
Сертификат Клиента	УСЦ обеспечивает доступ к сертификату для других Пользователей. Сертификат доступен после его создания

УСЦ публикует информацию о статусе сертификата в соответствии с Регламентом УСЦ, п. 4.4.9.

2.6.2 Периодичность предоставления информации

Обновления Веб-сайта УСЦ осуществляются в соответствии с Регламентом УСЦ, п. 8. Изменения в договорах УСЦ с Клиентом и УСЦ с уполномоченным лицом предоставляются на Веб-сайте УСЦ. Информация о статусе сертификата предоставляется на Веб-сайте УСЦ.

2.6.3 Контроль доступа на предоставление информации УСЦ

Информация, которая публикуется на Веб-сайте УСЦ, является общедоступной. Доступ для чтения этой информации не ограничен. УСЦ не требует оговаривать в договоре с уполномоченными лицами условия доступа к сертификатам, к информации о статусе сертификата, к спискам отозванных сертификатов. УСЦ обеспечивает защиту от несанкционированного доступа к базе данных сертификатов УСЦ.

2.6.4 База данных УСЦ

См. Регламент УСЦ, п. 2.1.5

2.7 Проверка работоспособности УСЦ

Проверка работоспособности УСЦ выполняется по утвержденной методике, разработанной Центральным удостоверяющим органом. УСЦ выполняет проверку работоспособности Регистрационного центра.

2.7.1 Частота проверки работоспособности УСЦ

Частота проверки работоспособности УСЦ выполняется по инструкции, прилагаемой к утвержденной методике.

2.7.2 Идентификация и уровень квалификации проверяющей организации

Проверка выполняется независимой организацией, которая имеет разрешение на проведение соответствующих работ:

- имеет опыт работы в технологиях инфраструктуры открытого ключа, владеет технологиями и механизмами защиты информации;
- является аккредитованной организацией, которая имеет соответствующую лицензию.

2.7.3 Взаимоотношения проверяющей организации с Клиентом

Проверяющая организация должна быть юридически и финансово независимой от УСЦ, а также от Клиентов.

2.7.4 Список разделов, не подлежащих проверке

Не предусмотрено

2.7.5 Меры при выявлении ошибок методики проверки работоспособности

Методика проверки работоспособности УСЦ составляется руководством УСЦ и Центральным удостоверяющим органом. Если обнаружены ошибки в методике проверки во время ее выполнения, руководство УСЦ отвечает за ход и оформление выполнения корректной методики проверки.

О выявлении ошибок в методике проверки работоспособности Украинский сертификационный центр сообщает в Центральный удостоверяющий орган. Методика корректной проверки работоспособности работы утверждается в течение 30 календарных дней и выполняется в течение указанного в ней периода времени. Руководство УСЦ определяет количество проверок, согласно утвержденным методикам и составляет соответствующий календарный план.

2.7.6 Предоставление результатов проверки

Результаты выполнения проверки УСЦ предоставляются по усмотрению руководства УСЦ.

2.8 Конфиденциальность и секретность

2.8.1 Типы информации, которые являются конфиденциальной

- данные заявок УСЦ, которые подаются в Центральный удостоверяющий орган;
- данные заявки Клиента на сертификат (см. п. 2.8.2);

- данные Договора УСЦ с Пользователем;
- данные результатов проверки, выполняемой УСЦ или Центрального удостоверяющего органа;
- данные об аварийных ситуациях УСЦ;
- данные о работе программного обеспечения, оборудования УСЦ
- сведения о порядке функционирования комплексной системе защиты и работе службы защиты информации УСЦ.

2.8.2 Типы информации, которые не конфиденциальны

Сертификаты, отозванные сертификаты, информация о статусе сертификата, база данных сертификатов УСЦ не являются конфиденциальной информацией. Информация, кроме разделов, приведенных в п.2.8.1, не является конфиденциальной.

2.8.3 Предоставление информации об отозванных или заблокированных сертификатах См. п. 2.8.2 Регламента УСЦ

2.8.4 Официальное требование выдачи информации конфиденциального характера по закону

Официальное требование выдачи информации происходит в случаях, предусмотренных законодательством Украины.

2.8.5 Обстоятельства, при которых предоставляются документы

УСЦ предоставляет конфиденциальную информацию в случае необходимости предоставления этой информации для судебного, административного процесса. Процесс предоставления документов осуществляется при следующих административных или гражданских мерах воздействия: вызов в суд, вызов на допрос, запрос на допуск к конфиденциальным документам, запрос на обработку документов. К этому разделу применяется политика секретности.

2.8.6 Раскрытие информации по требованию Клиента

Политика секретности УСЦ заключается в предоставлении Клиенту по его запросу конфиденциальной информации, относящейся к Клиенту. К этому разделу применяется политика секретности.

2.8.7 Обстоятельства, при которых предоставляется информация

Информация о сертификате, отозванных сертификатах, информация о статусе сертификата, база данных сертификатов УСЦ не являются конфиденциальной информацией и предоставляется Украинским сертификационным центром круглосуточно. Конфиденциальная информация предоставляется согласно п.п. 2.8.4, 2.8.5, 2.8.6.

2.9 Права на интеллектуальную собственность

Распределение прав на интеллектуальную собственность среди сотрудников УСЦ отличаются от прав Клиентов и уполномоченных лиц, что оговорено в договоре сотрудников УСЦ. Ниже описываются права на интеллектуальную собственность для Клиентов и уполномоченных лиц.

2.9.1 Права на сертификаты и информацию о списках отозванных сертификатов

УСЦ поддерживает все права на интеллектуальную собственность в сертификатах и списках отозванных сертификатов, которые они издадут.

2.9.2 Права на спецификацию политики безопасности сертификатов

УСЦ поддерживает все права на интеллектуальную собственность в соответствии с Регламентом УСЦ.

2.9.3 Права на имена

Клиент сертификата сохраняет право на имя или торговую марку компании, включенную в его заявку на сертификат и на имя в изданном сертификате.

2.9.4 Права на ключи и на данные о ключах

Пара ключей, соответствующая сертификату Клиента, является собственностью Клиента.

3 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1 Начальная регистрация

3.1.1 Типы имен

Во всех сертификатах, издаваемых Украинским сертификационным центром, используются имена, определенные стандартом X.500 «Information technology — Open Systems Interconnection — The Directory: Overview of Concepts, Models, and Services Recommendation X.500 ISO/IEC 9594-1».

3.1.1.1 Сертификаты УСЦ

В корневых сертификатах Украинского сертификационного центра используются следующие реквизиты полей:

- Страна (countryName)
- Город (localityName) Киев
- Организация (organizationName)
- Подразделение (organizationalUnitName)
- Полное имя (commonName)

В сертификатах Украинского сертификационного центра помимо перечисленных реквизитов могут использоваться дополнительные реквизиты.

3.1.1.2 Клиентские сертификаты УСЦ

Реквизиты Клиента определяются правилами использования определенного типа сертификата и договором с Клиентом.

3.1.2 Понятность имен

Все реквизиты, используемые в полях «Издатель» и «Владелец», должны быть понятными и легко устанавливать идентичность Издателя и Клиента сертификата. Псевдонимы и сокращения не используются при заполнении полей сертификата.

3.1.3 Правила интерпретации разных форм имен

Не устанавливаются.

3.1.4 Уникальность имени

Поле «Издатель» является уникальным во всех сертификатах, созданных Украинским сертификационным центром. В случае необходимости Украинский сертификационный центр может добавлять реквизит «дополнительный квалификатор» для обеспечения уникальности этого поля.

3.1.5 Разрешение споров, связанных с использованием имен

Украинский сертификационный центр имеет право отозвать или заблокировать сертификат в случае возникновения каких-либо споров, связанных с использованием имен и реквизитов в данном сертификате, информируя об этом Клиента непосредственно или через Регистрационный центр.

3.1.6 Процедура распознавания, аутентификации и роль торговой марки

См. раздел 3.1.5.

3.1.7 Проверка факта обладания секретным ключом

Украинский сертификационный центр проверяет факт существования секретного ключа и его соответствие открытому ключу, предоставленному Клиентом в составе заявки на сертификат. Эта проверка выполняется только после установления идентичности Клиента. В качестве заявки на сертификат может использоваться заявка на сертификат в формате PKCS#10 (Клиента или Регистрационного центра) или корневой сертификат версии 1.

3.1.8 Аутентификация подлинности организации

Украинский сертификационный центр гарантирует подлинность реквизитов организации и всех других данных, включенных в сертификат этой организации. Кроме того, проверяется факт обладания секретным ключом (см. п. 3.1.7).

3.1.8.1 Аутентификация подлинности организации Клиента

Для проверки аутентичности данных, включенных в заявку на сертификат, Украинский сертификационный центр требует от Клиента нотариально заверенных документов, подтверждающих соответствие этих данных. Представитель организации, подающий заявку на сертификат от имени организации, должен иметь доверенность на выполнение этой операции, оформленную в установленном порядке.

Перечень необходимых документов определяется п. 4.16 Правил усиленной сертификации и договором с организацией.

3.1.8.2 Аутентификация подлинности УСЦ

Обработка заявок на сертификат и создание сертификатов выполняется квалифицированным персоналом Украинского сертификационного центра по установленным правилам, которые предусматривают участие, по крайней мере, двух сотрудников УСЦ на каждом этапе создания сертификата.

3.1.9 Аутентификация персональных данных Клиента

Клиент должен предъявить документ, устанавливающий его личность. Для проверки соответствия персональных данных, включенных в заявку на сертификат, Украинский сертификационный центр требует от Клиента нотариально заверенных документов, подтверждающих верность всех таких данных.

Перечень необходимых документов определяется п. 4.16 Правил усиленной сертификации и договором с Клиентом.

3.2 Порядок повторной выдачи ключей или обновления сертификата

Украинский сертификационный центр не восстанавливает сертификаты Клиента в случае их отзыва или окончания срока действия и не продлевает срок действия актуальных сертификатов. В этих случаях Клиент должен обратиться за получением нового сертификата.

3.3 Повторная выдача ключей после отзыва сертификата

См. раздел 3.2.

3.4 Заявка на отзыв сертификат

Основанием для отзыва сертификата Клиента является заявка на отзыв сертификата. Эта заявка подается либо Клиентом, отзывающим сертификат, либо Регистрационным центром, который зарегистрировал заявку на сертификат, подлежащий отзыву. Регистрационный центр может подать такую заявку от имени Клиента или по своей инициативе в случаях,

предусмотренных договором Клиента с УСЦ. УСЦ принимает только заявки на отзыв сертификата, законность которых УСЦ может установить путем проверки цифровой подписи Регистрационного центра или Клиента или путем запроса пароля отзыва сертификата.

4 ПОРЯДОК ИЗДАНИЯ СЕРТИФИКАТОВ

4.1 Создание заявки на сертификат

Для получения сертификата Клиент создает заявку на сертификат. В заявку на сертификат включаются общие и дополнительные данные, которые определяют Клиента. Содержание этих данных определяется договором. Эти данные окончательны и в дальнейшем не изменяются.

Если эти данные неверны или неполны, то заявка отклоняется, и сертификат не формируется. Клиент вычисляет пару ключей с использованием любого алгоритма, поддерживаемого Украинским сертификационным центром. Вычисленный открытый ключ помещается в заявку на сертификат. Эта структура данных подписывается секретным ключом Клиента, отвечающим открытому ключу, включенному в заявку.

Заявка на сертификат Клиента предоставляется в Регистрационный центр или в Украинский сертификационный центр. Регистрационный центр или Украинский сертификационный центр проверяют данные Клиента и факт обладания секретным ключом(см.3.1.5). После принятия заявки, Регистрационный центр подписывает заявку своим секретным ключом и передает ее в Украинский сертификационный центр.

Украинский сертификационный центр гарантирует сохранение конфиденциальности данных, включенных в заявку на сертификат до момента создания сертификата. По просьбе Клиента Регистрационный центр или Украинский сертификационный центр могут вычислить пару ключей и создать заявку на сертификат на основании документов, предоставленных клиентом или его уполномоченным лицом, в этом случае они гарантируют конфиденциальность секретного ключа Клиента.

4.2 Создание сертификата Клиента

Сертификаты Клиента создаются на основе заявок на сертификат. Эти сертификаты подписываются секретным ключом УСЦ. Эту операцию выполняют уполномоченные сотрудники Украинского сертификационного центра. Формирование сертификата Клиента выполняется только в случае успешного исхода проверок, предусмотренных разделами 3.1.8 или 3.1.9 и 3.1.7. Проверяется цифровая подпись Регистрационного центра.

После принятия заявки УСЦ вносит в сертификат собственные идентификационные данные, срок действия сертификата, уникальный серийный номер сертификата, вносит в сертификат набор расширений, определяемых в договоре с Пользователем, и подписывает сертификат, проверяет правильность данных, фактически включенных в сертификат и правильность вычисленной цифровой подписи. Если сертификат вычислен без ошибок, то он вносится в базу данных. Сертификат Клиента может экспортироваться в двоичном виде или текстовом виде в формате Base64. Возможен экспорт сертификата Клиента и сертификатов УСЦ в одном блоке данных.

4.3 Принятие сертификата

Сертификат передается непосредственно Клиенту или через Регистрационный центр. Если Клиент принимает полученный сертификат, то сертификат вступает в силу после первого обновления списка отозванных сертификатов, следующего за моментом получения согласия Клиента. Для публикации сертификата необходимо согласие Клиента.

4.4 Блокирование и отзыв сертификата

4.4.1 Обстоятельства для отзыва сертификата

4.4.1.1 Обстоятельства для отзыва сертификата Клиента

Сертификат Клиента отзывается при:

- компрометации секретного ключа Клиента;
- нарушении условий договора Клиентом;
- истечении срока действия договора;
- нарушениях Клиентом положений Регламента УСЦ;
- изменении реквизитов Клиента, включенных в его сертификат;
- если обнаружится, что данные, включенные в сертификат, не отвечают действительности;
- если сертификат был издан без согласия Клиента;
- в случае ликвидации организации или смерти Клиента.

Отзыв сертификата производится согласно разделу 3.4. Клиент обязан немедленно информировать Украинский сертификационный центр о компрометации секретного ключа.

4.4.1.2 Обстоятельства для отзыва сертификата УСЦ

Сертификат УСЦ отзывается при:

- компрометации секретного ключа УСЦ;
- нарушении положений Регламента УСЦ;
- по инициативе уполномоченных сотрудников Украинского сертификационного центра.

4.4.2 Кто может отозвать сертификат

4.4.2.1 Кто может отозвать сертификат Клиента

Подать заявку на отзыв сертификата Клиента могут:

- Клиент-владелец сертификата;
- Регистрационный центр, который зарегистрировал заявку на создание сертификата Клиента;
- Украинский сертификационный центр.

4.4.2.2 Кто может отозвать сертификат УСЦ

Отозвать сертификат УСЦ может УСЦ или Центральный удостоверяющий орган согласно его регламенту работы.

4.4.3 Процедуры отзыва сертификата Клиента

4.4.3.1 Процедура отзыва сертификата Клиента

В случае возникновения обстоятельств, требующих отзыва сертификата Клиента, Клиент или Регистрационный центр должны направить в Украинский сертификационный центр заявку на отзыв сертификата и Украинский сертификационный центр отзывает сертификат Клиента согласно п. 3.4.

4.4.3.2 Процедура отзыва сертификата УСЦ

В случае возникновения обстоятельств, требующих отзыва сертификата УСЦ, Украинский сертификационный центр производит отзыв сертификата УСЦ согласно внутренним документам УСЦ.

4.4.4 Период отсрочки отзыва сертификата

УСЦ начинает обработку заявки на отзыв сертификата немедленно после установления законности заявки согласно п. 3.4. После установления законности заявки на отзыв сертификата период отсрочки отзыва сертификата определяется техническими возможностями программных и аппаратных средств УСЦ, участвующих в обработке заявки.

4.4.5 Обстоятельства, при которых сертификат может быть заблокирован

Обстоятельства, при которых допускается блокирование сертификата, определяются договором с Клиентом.

4.4.6 Кто может заблокировать сертификат

Подать заявку на блокирование сертификата Клиента могут:

- Клиент-владелец сертификата;
- Регистрационный центр, который зарегистрировал заявку на создание сертификата Клиента в случаях, предусмотренных договором Клиента с УСЦ;
- Украинский сертификационный центр;

4.4.7 Процедуры, используемые для блокирования сертификата

В случае возникновения обстоятельств, требующих блокирования сертификата Клиента, Клиент или Регистрационный центр должны направить в Украинский сертификационный центр заявку на блокирование сертификата. Такая заявка обрабатывается согласно п. 3.4 и 4.4.4.

4.4.8 Ограничения для периода блокирования сертификата

Период блокирования сертификата Клиента не превышает 3 месяцев. По истечении этого срока заблокированный сертификат отзывается.

4.4.9 Частота формирования списка отозванных сертификатов

Список отозванных сертификатов обновляется ежедневно. В список отозванных сертификатов не включаются сертификаты, срок действия которых истек к моменту обновления списка отозванных сертификатов.

4.4.10 Правила использования списка отозванных сертификатов Клиентами УСЦ

Не устанавливаются.

4.4.11 Возможность получения информации о статусе сертификата в реальном времени

Украинский сертификационный центр предоставляет круглосуточную возможность проверки состояния сертификатов в режиме реального времени.

4.4.12 Правила использования клиентом информации о состоянии сертификата в режиме реального времени

Не устанавливаются.

4.4.13 Наличие дополнительных способов оповещения об отзыве сертификатов

Не предусмотрены. См.4.4.7

4.4.14 Правила использования Пользователями дополнительных способов оповещения об отзыве сертификатов

Не устанавливаются. См.4.4.7

4.4.15 Особые требования к действиям УСЦ при компрометации секретного ключа УСЦ

Украинский сертификационный центр использует все имеющиеся технические возможности для оповещения своих Пользователей о компрометации секретного ключа УСЦ.

4.5 Процедуры контроля защиты

4.5.1 Виды записанных событий

К записанным событиям относится протоколирование работы всех программных средств, работающих в УСЦ, которые имеют доступ к базе данных. Протоколирование ведется в выделенную таблицу в базе данных, а также в локальный файл на каждом рабочем месте или сервере. Протоколирование ведется по событиям:

- Генерация ключей, формирование сертификатов, списков отзыванных сертификатов, отзыв сертификатов, отметок времени, данных текущего состояния сертификата и других объектов базы данных УСЦ;
- Обслуживание всех типов заявок в УСЦ;
- Начало и окончание работы программных средств, операторов, администраторов, серверов УСЦ;
- Ошибки, предупреждения и сбои в работе программных средств и серверов УСЦ;
- замене технических средств в программно-техническом комплексе (далее - ПТК);
- техническом обслуживании ПТК УСЦ;
- попытках создания, уничтожения, установления пароля, изменения прав доступа, системных привилегий и прочее в ПТК УСЦ;
- попытки несанкционированного доступа к ПТК УСЦ;
- предоставление доступа к ПТК персоналу УСЦ;
- сбои в работе, техническое обслуживание, изменение системной конфигурации ПТК.

Протокольная запись содержит данные:

- Дата и время;
- Тип сообщения;
- Сообщение;
- Дополнительную информацию;
- IP адрес и другую справочную информацию о программном средстве (только для протокольной записи в базе данных);

4.5.2 Периодичность процесса записи события

Процесс записи протокольного события инициируется сразу же, после его появления. Запись производится в базу данных и на жесткий диск в локальный файл. Записи в базу данных и на диск идентичны.

4.5.3 Срок хранения журналов

Срок хранения протокольных записей не ограничен, но не менее 2-х лет (п.5.13 Правил). Для автоматического удаления протокольных записей из базы данных возможно использование программных средств, а также возможно удаление записей из базы данных вручную администратором базы данных.

4.5.4 Защита журналов

Протокольные записи в базе данных доступны к удалению только администратором базы данных, после прохождения соответствующей регистрации на сервере базы данных.

4.5.5 Резервное копирование журнала

Вся база данных УСЦ, вместе с системными таблицами, копируется в виде бинарного файла на жесткий диск администратора базы данных, а затем на оптический компакт диск один раз в сутки.

4.5.6 Тип системы ведения журналов аудита (встроенная/внешняя)

В УСЦ применяется автоматическая система протоколирования работы всех программных средств.

4.5.7 Система оповещения Клиентов о компрометации секретного ключа

Согласно 4.4.15.

4.5.8 Анализ безопасности УСЦ

Производится администратором базы данных и администратором безопасности при разборе записей протоколирования работы всех программных средств УСЦ.

4.6 Архивация

4.6.1 Виды записанных событий

Архивация предусматривает сохранение всей базы данных УСЦ, которая содержит полную информацию в электронном виде о работе УСЦ.

4.6.2 Срок хранения архива

Срок хранения архива УСЦ не ограничен.

4.6.3 Защита архива

Создать архив может администратор базы данных УСЦ, после соответствующей аутентификации на сервере базы данных. Оптические носители с архивами базы данных администратор безопасности хранит в сейфе.

4.6.4 Процедура создания резервной копии архива

Фиксируется ежесуточное состояние базы данных УСЦ. Резервное дублирование суточных версий не предусматривается.

4.6.5 Требования фиксации времени создания записей в архиве

Создание каждой записи в базе данных УСЦ фиксируется датой и временем с точностью до секунды.

4.6.6 Описание системы архивации (встроенная/внешняя, доступ и т.д.)

Система архивации базы данных осуществляется стандартными средствами экспорта данных из системы управления базы данных (СУБД).

Хранение всех сформированных УСЦ сертификатов осуществляется в эталонной, резервной и архивной базах УСЦ.

4.7 Плановая замена ключей

Срок действия сертификатов Украинского сертификационного центра и отвечающих им секретных ключей - 5 лет. Срок действия сертификатов Пользователей в общем случае не превышает 2 лет. За год до окончания срока действия сертификата Украинского сертификационного центра создается новый сертификат Украинского сертификационного центра и используется при создании новых клиентских сертификатов. Старый сертификат изымается из использования. Таким образом, плановая замена ключей Украинского сертификационного центра происходит незаметно для Пользователей УСЦ.

4.8 Действия в аварийной ситуации или при компрометации ключа УСЦ

Украинский сертификационный центр использует комплексную систему обеспечения надежности и безопасности функционирования всех аппаратных и программных средств УСЦ, которые сводят к минимуму риск нарушения нормальной работы центра и компрометации ключевых данных. На случай возникновения чрезвычайной ситуации УСЦ реализовывает мероприятия соответствии с планом действий в чрезвычайной ситуации, который обеспечивает восстановление нормальной работы УСЦ в максимально короткий срок.

4.8.1 Порча оборудования, программного обеспечения или искажение данных

В случае отказа оборудования или программных средств, специальная группа специалистов УСЦ анализирует ситуацию и принимает адекватные меры по восстановлению работоспособности центра. В случае необходимости выполняется восстановление работоспособности УСЦ согласно

разделу 4.8.2. Если обстоятельства требуют отзыва сертификатов УСЦ, то восстановление работоспособности УСЦ выполняется согласно разделу 4.8.3.

4.8.2 Восстановление работоспособности УСЦ в случае аварии

В случае аварии работоспособность Украинского сертификационного центра восстанавливается в течение одних суток при помощи инсталляции и настройки работы серверов, базы данных и программных средств УСЦ на новых аппаратных средствах; путем копирования в систему последней архивированной (сохраненной) версии базы данных УСЦ.

4.8.3 Восстановление работоспособности УСЦ в случае компрометация ключа

В случае компрометации ключа УСЦ Украинский сертификационный центр немедленно отзывает такой сертификат и немедленно извещает Пользователей об этом, используя все имеющиеся технические возможности. После установления причин компрометации и принятия мер по их устранению Украинский сертификационный центр заново создает ключи и сертификаты УСЦ. После восстановления работоспособности Украинский сертификационный центр бесплатно создает новые сертификаты всем Клиентам УСЦ.

4.9 Прекращение деятельности УСЦ

О решении относительно прекращения деятельности УСЦ, Украинский сертификационный центр сообщает Клиенту за три месяца. Архивы УСЦ передаются на хранение в органы местной власти в случае возникновения судебных разбирательств между Украинским сертификационным центром и Клиентами.

Клиент имеет право избрать по собственному желанию любой центр сертификации ключей для дальнейшего обслуживания.

5 КОНТРОЛЬ ЗАЩИТЫ ОБОРУДОВАНИЯ УСЦ, ПРОЦЕССА РАБОТЫ ЭТОГО ОБОРУДОВАНИЯ И ПЕРСОНАЛА

5.1 Физический контроль

5.1.1 Конструкция и размещение рабочих мест

База данных на жестких магнитных дисках представляет собой отдельный сервер “SmartStorage 170”, узел кластера из двух серверов “SmartServer SR-520”, сервер обработки и транспорта объектов, сервер открытого доступа (два сервера “SmartServer SR-130”), KVM-переключатель ATEN ACS-1208A, коммутатор “Baseline Svitch 2226”. Коммутационная аппаратура локальной сети, а также рабочее место системного администратора смонтировано в специальном металлическом шкафу, который установлен в отдельной кабине. Кабина расположена внутри специального помещения УСЦ.

Кабина и шкаф снаряжены замками, ключи от которых хранятся в сейфе администратора сертификации, который несет ответственность за использование личного ключа УСЦ, копии ключей хранятся в сейфе администратора безопасности.

Рабочие станции администратора сертификации, оператора сертификации установлены в специальном помещении УСЦ. Они подключены к радиальным экранированным линиям структурированной кабельной системы, которые выходят из шкафа серверов.

Для генерации личных ключей используется отдельная рабочая станция (персональный компьютер, отделенный от сети других средств программно-аппаратного комплекса), на которой установлены специальные программные средства.

5.1.2 Физический доступ

Украинский сертификационный центр находится на шестом этаже семиэтажного здания, вход ограничен системой пропусков. Единый вход к помещению УСЦ оснащен замками, сигнализацией открытой двери, а собственное помещение – сигнализацией движения и разбивке

стекла, которые объединены принимающим контрольным прибором с кодовым пультом. Помещение находится под охраной (ДЗАТ “Охрана-комплекс”).

Доступ к УСЦ имеют персонал Украинского сертификационного центра.

5.1.3 Кондиционирование воздуха и электрическое питание

В помещении УСЦ встроена кабина для шкафа серверов и отдельная комната для рабочих мест персонала УСЦ. Кабина и комната оснащена кондиционерами.

Все средства аппаратно-технического комплекса обеспечены устройствами беспереывного питания: “APC Smart-UPS 2U 3000VA” (2 комплекта в шкафу серверов), “APC Back-UPS RS800” (по одному комплекту на рабочую станцию).

5.1.4 Уровень влажности

В помещении УСЦ система водоснабжения не предусмотрена. Влажность воздуха контролируется с помощью влагомера.

5.1.5 Обеспечение противопожарной защиты

Помещение УСЦ обеспечено противопожарной безопасностью.

5.1.6 Уровень шума

Основными источниками шума в помещении УСЦ являются вентиляторы охлаждения серверов, рабочих станций и кондиционеров. Для охлаждения серверов, в кабине установлен кондиционер, для уменьшения уровня шума в кабине установлена шумоизоляционная дверь.

5.1.7 Утилизация отходов

Вся информация о работе УСЦ хранится в электронном виде в базе данных. Утилизация отходов не предусматривается.

5.1.8 Сохранение архивов вне УСЦ

Архивы УСЦ не передаются на хранение другим организациям и частным лицам.

5.2 Процедурный контроль

5.2.1 Доверенные роли

В структуре УСЦ предусмотрены должности: директор, администратор безопасности, администратор сертификации, оператор сертификации, системный администратор.

В обязанности администратора безопасности входит:

- обеспечение полноты и качественного выполнения организационно-технических мероприятий по защите информации;
- разработка распорядительных документов по обеспечению защиты информации;
- своевременное реагирование на попытки несанкционированного доступа к ресурсу программно-технического комплекса УСЦ;
- участие в генерации ключей УСЦ и должностных лиц УСЦ, участие в формировании сертификатов ключей должностных лиц УСЦ;
- контроль за хранением личного ключа УСЦ и его резервной копии, личных ключей должностных лиц УСЦ;
- участие в уничтожении личного ключа УСЦ, контроль за своевременным уничтожением личных ключей должностных лиц УСЦ;
- обеспечение функционирования комплексной системы защиты информации;
- обеспечение организации и проведения мероприятий по оперативному восстановлению функционирования комплексной системы защиты информации после сбоев, отказов, аварий программно-технического комплекса;
- ведения журнала учета администратора безопасности.

В основные обязанности администратора сертификации входит:

- предоставление в центральный удостоверяющий орган данных, необходимых для формирования сертификата открытого ключа УСЦ;
- обеспечение использования секретного ключа УСЦ во время формирования клиентских сертификатов открытых ключей, списков отозванных сертификатов, отметок времени и других объектов сертификации УСЦ;
- обеспечение ведения, архивации и восстановления эталонной базы сформированных сертификатов;
- предоставление администратору безопасности информации о событиях, которые влияют на безопасность функционирования УСЦ.

В основные обязанности оператора сертификации входит:

- прием документов организаций и лиц, которые обратились в УСЦ, с целью формирования сертификата регистрационного центра или сертификата Клиента;
- проверка данных, обязательных для формирования сертификата;
- создание и отзыв сертификатов;
- создание списков отозванных сертификатов;
- информирования администратора безопасности о событиях, которые влияют на безопасность функционирования УСЦ.

Основные обязанности системного администратора:

- организация эксплуатации и технического обслуживания программно-технического комплекса УСЦ;
- обеспечение актуальности эталонных, архивных и резервных копий баз сертификатов УСЦ и их хранение;
- обеспечение поддержки электронного информационного ресурса УСЦ;
- администрирование средств программно-технического комплекса УСЦ;
- участие в внедрении и обеспечении функционирования комплексной системы защиты информации УСЦ;
- обеспечение резервного копирования (архивирования) базы данных УСЦ, общесистемного и специального программного обеспечения программно-технического комплекса УСЦ;
- ведение журналов аудита событий, регистрируемых программно-техническим комплексом УСЦ.

5.2.2 Требуемое количество людей для выполнения определенного задания

Для обеспечения непрерывной работы УСЦ, с соблюдением надлежащей оперативности, число операторов сертификации и пунктов регистрации зависит от количества Клиентов. Эти показатели оцениваются из реестра обращений Клиентов за единицу времени. При подаче Пользователями менее 100 заявок на сертификацию ключей их обслуживание может осуществлять один оператор сертификации. При подаче более 100 заявок в сутки, количество операторов рассчитывается по следующей формуле: количество операторов = количество заявок Пользователей / 100.

5.2.3 Идентификация и аутентификация человека для каждой роли

Для каждого должностного лица, которое использует в работе программные средства УСЦ, создается пара ключей (секретный и открытый). При помощи сертификата открытого ключа должностного лица на рабочем месте обеспечивается аутентификация, предоставляется доступ к необходимой информации, обеспечивается целостность и конфиденциальность данных, которые обрабатываются в Украинском сертификационном центре.

5.3 Требования к персоналу УСЦ

5.3.1 Требования по знаниям, уровню квалификации, опыту и категории допуска

К работе с программными средствами УСЦ допускаются должностные лица, которые изучили соответствующую эксплуатационную документацию и предупреждены об ответственности за разглашение конфиденциальной информации.

5.3.2 Основы процедуры проверки

Предусматривается испытательный срок для должностного лица, который изучил документы, в соответствии с п. 5.3.1, 5.3.3.

5.3.3 Требования по обучению персонала

Обучение персонала состоит из изучения законодательной и нормативной базы законодательства Украины, изучения Регламента УСЦ, должностных обязанностей, эксплуатационной документации.

5.3.4 Частота переобучения и требования по переобучению

Необходимость переобучения появляется в случаях изменения должностных обязанностей, необходимости дублирования функций другого должностного лица, изменениях в программно-техническом комплексе. Процедура переобучения подобна процедуре обучения.

5.3.5 График работы

Круглосуточное обслуживание Пользователей УСЦ обеспечивается непрерывной работой серверов УСЦ. Обслуживание заявок Пользователей на сертификацию открытого ключа производится операторами сертификации в соответствии с графиком работы должностных лиц УСЦ.

5.3.6 Санкции за неправомерные действия

За неправомерные действия или нарушение политики безопасности сертификата, персонал УСЦ несет административную ответственность в соответствии с законодательством Украины.

5.3.7 Требования по заключению контракта с персоналом

При приеме на работу в УСЦ кандидат предъявляет документы о высшем техническом образовании. Кандидат должен иметь стаж работы по специальности не менее 5 лет.

5.3.8 Доступ к документации УСЦ

Для каждого должностного лица предоставляется должностная инструкция. Для должностного лица, работающего с программными средствами УСЦ, предоставляется эксплуатационная документация.

6 ТЕХНИЧЕСКИЙ КОНТРОЛЬ ЗАЩИТЫ

6.1 Установка программного обеспечения и генерация пары ключей

6.1.1 Генерация пары ключей

Для создания секретных ключей УСЦ используется отдельная рабочая станция (персональный компьютер, отделенный от сети других программно-аппаратных средств комплекса), на которой установлены специальные программные средства, на которые выдан документ соответствия. Создание ключей УСЦ осуществляется должностными лицами. Процесс создания ключей протоколируется должностными лицами, которые брали участие в этом процессе.

6.1.2 Доставка секретного ключа Клиенту

Пара ключей Клиента создаются самим Клиентом или УСЦ по желанию Клиента.

Созданные в УСЦ ключи Клиентов в УСЦ не хранятся, а передаются Клиенту сразу после создания заявки на сертификат. Формат передаваемых секретных ключей определяется договором УСЦ с Клиентом.

6.1.3 Доставка открытого ключа Издателю сертификата

Клиенты подают на рассмотрение свой открытый ключ в Украинский сертификационный центр для электронной сертификации в составе заявки на сертификат. в формате.

6.1.4 Доставка открытого ключа Клиенту

УСЦ передает свой открытый ключ Клиентам в составе сертификатов УСЦ, либо непосредственно Клиенту, либо через Регистрационный центр.

6.1.5 Размеры ключа

УСЦ использует такие размеры секретных ключей цифровой подписи УСЦ.

Алгоритм	Размер секретного ключа в битах	Стойкость алгоритма
ДСТУ 4145-2002	не менее 257	не менее 10^{37}
ГОСТ 34.310-95	256	10^{24}
Р 34.10-2001	256	10^{37}
DSA	160	10^{24}
RSA	1024	10^{24}
ECDSA	не менее 163	не менее 10^{24}

УСЦ рекомендует своим Клиентам использовать ключи таких же размеров.

6.1.6 Параметры генерации открытого ключа

УСЦ самостоятельно вычисляет параметры создания ключей в полном соответствии с требованиями стандартов, которые определяют свойства таких параметров, во всех тех случаях, когда алгоритм вычисления пары ключей требует наличия параметров.

6.1.7 Проверка качества параметров генерации ключей

УСЦ проводит полную проверку соответствия параметров создания ключей требованиям стандартов, которые определяют алгоритм вычисления пары ключей, во всех тех случаях, когда алгоритм вычисления пары ключей требует наличия параметров.

6.1.8 Программное обеспечение для генерации пары ключей

УСЦ создает свою пару ключей в программных криптографических модулях в соответствии с Регламентом УСЦ, п.6.2.1. Пара ключей Клиента может быть создана с помощью программного обеспечения Клиента.

6.1.9 Назначение ключа

Для ограничения сферы использования ключей УСЦ использует расширения «использование ключа» и «уточнение использования ключа».

6.2 Защита секретного ключа

УСЦ выполняет совмещенный физический, логический и процедурный контроль для защиты секретного ключа УСЦ. Логический и процедурный контроль описан в п. 6.5, 6.6. Физический контроль доступа описан в п. 5.1. Клиент обязан, согласно договору, выполнять необходимые меры предохранения во избежание потери, использования ключа после окончания его срока действия или неразрешенного использования секретного ключа.

6.2.1 Стандарты для криптографических модулей

УСЦ использует программное обеспечение с криптографическими модулями, соответствующее «Правилам усиленной сертификации» утвержденным приказом ДСТСЗИ СБУ Украины №3 от 13.01.2005 .

6.2.2 Доступ к секретному ключу УСЦ

В УСЦ применяются разделенный доступ авторизованных лиц к секретному ключу УСЦ по схеме 2 из m , $m > 2$.

6.2.3 Возможность предоставления доступа к секретному ключу посторонним организациям

Не предусмотрена.

6.2.4 Создание копий секретного ключа

УСЦ создает резервные копии секретного ключа УСЦ для его восстановления в случае аварийного сбоя. Секретные ключи УСЦ хранятся в зашифрованном виде вместе с программным криптографическим модулем на носителях данных. Криптографические модули применяются для получения секретного ключа УСЦ, соответственно требованиям Регламента УСЦ, п.6.2.1. секретный ключ копируется в архив вместе с программным криптографическим модулем, в соответствии с п. 6.2.6, Регламента УСЦ. Носители данных содержат резервные копии секретного ключа УСЦ, соответствующие требованиям Регламента УСЦ, п. 5.1, 6.2.1. УСЦ сертификационный центр не сохраняет, не резервирует и не архивирует секретный ключ Клиента.

6.2.5 Архивирование секретного ключа

При окончании срока действия созданной пары ключей УСЦ, эта пара ключей сохраняется в архиве на период, сроком 5 лет. Архивная копия этой пары ключей будет надежно храниться, используя носители данных, соответствующие Регламенту УСЦ, п. 6.2.1. Процедурный контроль защищает архивную пару ключей от ее восстановления. После окончания архивного периода (5 лет) ключей УСЦ, обеспечивается их уничтожение, в соответствии с Регламентом УСЦ, п. 6.2.9.

УСЦ не архивирует секретные ключи Клиента.

6.2.6 Введение секретного ключа в криптографический модуль

УСЦ создает пару ключей УСЦ при помощи программного криптографического модуля, в котором они будут использоваться в дальнейшем. УСЦ создает архивные копии пары ключей УСЦ для его восстановления в случае аварийного сбоя. Пара ключей сохраняется на носителе данных.

6.2.7 Метод активации секретного ключа

УСЦ защищает данные для восстановления его секретного ключа. Данные защищены от несанкционированного доступа и использования.

6.2.7.1 Секретный ключ Клиента

УСЦ рекомендует Клиенту использовать надежные механизмы защиты секретного ключа, например, использование микропроцессорной карточки (smart card), устройства биометрического доступа и другого оборудования для хранения секретного ключа, не допускающим его несанкционированное изменение, уничтожение или ознакомление с ним.

6.2.7.1.1 Сертификат с обычным уровнем защиты

УСЦ рекомендует Клиенту для защиты секретного ключа с обычным уровнем защиты применять меры для защиты его рабочего места от несанкционированного использования и активизации секретного ключа Клиента без его регистрации.

УСЦ рекомендует Клиенту использовать пароль, в соответствии с Регламентом УСЦ, п. 6.4.1 или использовать защиту от эквивалентного набора пароля при регистрации Клиента перед

началом срока действия ключа, который включает, например, пароль для входа в компьютер, пароль на защиту экрана, пароль на компьютер при сетевой работе Клиента.

6.2.7.1.2 Сертификат с повышенным уровнем защиты

УСЦ рекомендует для защиты секретного ключа Клиента с повышенным уровнем защиты использовать:

- Smart Card, другое устройство для криптографического программного обеспечения, устройство биометрического доступа, пароль или защиту от эквивалентного набора пароля при регистрации Клиента перед началом срока действия ключа;

- Необходимые меры для защиты его рабочего места от несанкционированного доступа или сервера и началом срока действия секретного ключа Клиента без его регистрации.

Использовать пароль вместе со Smart Card, другим устройством для криптографического программного обеспечения, устройством биометрического доступа, рекомендованным в соответствии с Регламентом УСЦ п. 6.4.1. При отключении устройства, секретный ключ будет сохранен только в зашифрованной форме.

6.2.7.2 Секретный ключ УСЦ

Секретный ключ УСЦ имеет ограниченный по времени срок действия. Ограничивается время начала работы секретного ключа и время окончания работы.

6.2.8 Метод блокирования секретного ключа

Секретный ключ УСЦ блокируется путем отзыва сертификата УСЦ.

Клиент может заблокировать свой секретный ключ после любого события. Для этого необходимо известить УСЦ, Регистрационный центр или направить заявку на отзыв сертификата в соответствии с данным Регламентом. У Клиента есть обязательства по защите своего секретного ключа в соответствии с Регламентом УСЦ, п. 2.1.3, 6.4.1.

6.2.9 Метод ликвидации секретного ключа

При окончании эксплуатационного срока службы УСЦ, одна или несколько копий секретного ключа УСЦ архивируется в соответствии с Регламентом УСЦ, п. 6.2.5. Архивированный секретный ключ УСЦ удаляется по окончании периода его архивного хранения. УСЦ ликвидирует свой секретный ключ надежным способом, который не позволяет восстановить этот ключ.

6.3 Другие аспекты управления парой ключей

6.3.1 Секретный архивный ключ

УСЦ и Клиент должны выполнять процедуру копирования и архивирования секретного ключа.

6.3.2 Период использования открытого и секретного ключа

Период действия сертификата заканчивается при окончании его срока действия или при его отзыве. Период действия пары ключей совпадают со сроком действия соответствующего сертификата. Граничный срок действия сертификатов отвечает п.27 Порядка аккредитации центра сертификации ключей согласно постановлению КМУ №903.

УСЦ должен закончить использование своей пары ключей после окончания срока их использования.

6.4 Данные для начала срока действия секретного ключа

6.4.1 Установка и создание данных для секретного ключа

Для начала использования секретного ключа необходимо ввести пароль для доступа к данным секретного ключа. Создание и сохранение секретного ключа протоколируется. УСЦ рекомендует, чтобы Клиент выбирал надежные пароли для защиты своего секретного ключа. УСЦ

рекомендует использовать механизмы регистрации для использования секретного ключа (т.е. символ и парольная фраза, биометрические данные и парольная фраза).

6.4.2 Защита данных секретного ключа

Требованием к УСЦ является: надежное хранение секретного ключа и подписание Договора, который подтверждает ответственность УСЦ.

УСЦ рекомендует, чтобы Клиент сохранял свой секретный ключ в зашифрованном виде, а для доступа к нему требовался: аппаратный символ или парольная фраза. УСЦ рекомендует Клиенту использовать механизмы регистрации для использования секретного ключа (т.е. символ и парольная фраза, биометрические данные и парольная фраза, биометрические данные и символ).

6.4.3 Другие аспекты для данных секретного ключа

См. п.п. 6.4.1, 6.4.2

6.5 Контроль компьютерной защиты

6.5.1 Специфика технических требований компьютерной защиты

Украинский сертификационный центр гарантирует, что программные средства УСЦ и файлы с данными, надежно защищены от несанкционированного доступа. Украинский сертификационный центр разграничивает доступ к базе данных сертификатов в соответствии с обязанностями персонала.

6.5.2 Уровень компьютерной защиты

Уровень компьютерной защиты должен соответствовать пункту 5.6 Правил усиленной сертификации.

6.6 Технический контроль жизненного цикла

6.6.1 Контроль развития системы

Приложения системы выполнены в соответствии с системой УСЦ и стандартами.

6.6.2 Контроль управления системой защиты

Украинский сертификационный центр использует механизмы управления системой защиты, определенные внутренними документами УСЦ.

6.7 Контроль сетевой системы защиты

УСЦ использует сетевую систему защиты информации, в соответствии с политикой безопасности УСЦ для защиты данных от несанкционированного доступа. Сетевая защита информации УСЦ осуществляется путем использования криптографических алгоритмов, электронной цифровой подписи и собственных протоколов доступа к базе данных для Пользователей.

6.8 Контроль построения криптографического модуля

Украинский сертификационный центр использует криптографический модуль, соответствующий требованиям, описанным в Регламенте УСЦ, п. 6.2.1

7 ПРОФИЛИ СЕРТИФИКАТА ОТКРЫТЫХ КЛЮЧЕЙ И СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ

Профили сертификата открытых ключей и списка отозванных сертификатов полностью соответствуют Правилам усиленной сертификации. Форматы данных и объектные идентификаторы, необходимые для нормального функционирования УСЦ и не охваченные Правилами усиленной сертификации, публикуются в отдельном документе.

8 РУКОВОДСТВО ПО РЕГЛАМЕНТУ

8.1 Процедура внесения изменений в Регламент

Дополнения к Регламенту вносятся руководством УСЦ. Дополнения оформляются в виде отдельных документов, содержащих дополнения или обновления пунктов. Все дополнения или обновления пунктов Регламента размещаются на Веб-сайте УСЦ.

Дополнения в регламент вносятся в порядке его согласования с контролирующим органом.

8.1.1 Пункты, которые можно изменять без уведомления

Украинский сертификационный центр может дополнять Регламент без уведомления Клиентов. К таким пунктам относятся орфографические и типографские ошибки.

8.1.2 Пункты, которые можно изменять с уведомлением

Украинский сертификационный центр может вносить дополнения в Регламент в соответствие с порядком, изложенным в п. 8.1.

8.1.2.1 Перечень пунктов, который можно изменять, но с уведомлением

Об внесенных в положения Регламента изменениях, касающихся имущественных взаимоотношений между УСЦ и Клиентами, УСЦ уведомляет Клиентов. В частности к таким положениям относится Договор между УСЦ и Клиентом.

8.1.2.2 Механизм уведомления

После внесения необходимых дополнений или обновлений в Регламент их размещают на Веб-сайте УСЦ.

8.1.2.3 Период комментария изменений

Не устанавливается.

8.1.2.4 Механизм трактовки комментария изменений

Не определяется.

8.2 Публикации и уведомления УСЦ

Веб-сайт УСЦ : <http://83.170.246.26>

8.3 Процедура утверждения Регламента

См. п. 8.1

9 УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И ОПРЕДЕЛЕНИЯ

9.1 Перечень условных обозначений

PKI – технология инфраструктуры открытого ключа (Public key infrastructure);

УСЦ – Украинский сертификационный центр;

РЦ – Регистрационный центр;

ISO 3166 (804) – международные стандарты;

ITU-T Recommendation X.509/ISO/IEC 9594-8 – международная рекомендации по организации инфраструктуры открытых ключей , сертификатов, объектов сертификации и другое;

RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

UTC - всемирное координированное время;

Веб-сайт – сервер, который работает по протоколу HTTP (hypertext transfer protocol);

Электронная почта – обмен электронными сообщениями при помощи сервера приема почты (протокол POP3/IMAP) и отправки почты (протокол SMTP);

TCP/IP – протокол обмена данными в сети Интернет/Интранет (transmission control protocol/internet protocol);

ДСТУ 4145-2002 „Информационная технология. Криптографическая защита информации. Электронная цифровая подпись, которая основывается на эллиптических кривых”- государственный стандарт Украины;

ГОСТ 34.310-95 „Информационная технология. Криптографическая защита информации. Процедуры создания и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма”- государственный стандарт СССР;

ГОСТ 34.311-95 „Информационная технология. Криптографическая защита информации. Функция хеширования” - государственный стандарт СССР;

DSA, RSA, ECDSA – FIPS PUB 186-2 DIGITAL SIGNATURE STANDARD (DSS)

ASN1 – синтаксис оформления кодированных структур данных;

PKCS#10 – PKCS #10 v1.7: Certification Request Syntax Standard

PKCS#7 – Cryptographic Message Syntax Standard;

Правила DER ITU-T Recommendation X.690 Information Technology - ASN.1 Encoding Rules - Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER);

СУБД - система управления базы данных;

CRL – список отозванных сертификатов (Certificate Revocation List).

9.2 Определения

Система «Сертификат» – программно-аппаратный комплекс Украинского сертификационного центра;

Сертификационный центр – юридическое лицо, предоставляющее услуги в сфере электронной цифровой подписи, в том числе по сертификации открытых ключей Клиентов;

Регистрационный центр (РЦ) – юридическое или физическое лицо, предоставляющее услуги регистрации заявок Клиента. Оператор РЦ идентифицирует Клиента с заявкой на сертификат открытого ключа, подписывает личным ключом РЦ заявку Клиента и доставляет заявку в УСЦ;

Пользователь – физическое или юридическое лицо, использующее сертификаты открытого ключа. Пользователь УСЦ необязательно является клиентом УСЦ;

Клиент – физическое или юридическое лицо, имеющее договорные отношения с УСЦ на получение услуг электронной цифровой подписи. Клиент УСЦ одновременно является пользователем УСЦ;

Уполномоченное лицо – физическое или юридическое лицо, которое уполномочено клиентом на получение сертификата;

Запрос на сертификат – просьба о получении ранее созданного сертификата;

Заявка на сертификат – закодированная последовательность данных, которая включает открытый ключ, персональные данные Пользователя, служебную информацию, электронную цифровую подпись Клиента и РЦ (может отсутствовать) на формирование нового сертификата открытого ключа;

Секретный ключ – индивидуальный параметр криптографического алгоритма, который должен храниться Клиентом в тайне;

Открытый ключ – индивидуальный параметр криптографического алгоритма, который в кодированном виде включается в сертификат открытых ключей;

Данные для активации сертификата - значения данных (кроме ключей), которые используются в криптографических модулях и требуют защиты (например, код, пароль, открытый ключ);

Сертификат УСЦ - сертификат открытого ключа, подписанный секретным ключом Украинского сертификационного центра, сертификат открытого ключа которого, подписан секретным ключом вышестоящего удостоверяющего органа или самого Украинского сертификационного центра;

Политика сертификата - установленный набор правил, который предписывает использование сертификата в тех или иных условиях, а также с использованием усиленных требований политики безопасности (усиленный сертификат);

Описание политики безопасности – описание политики безопасности, отвечающее объектному идентификатору политики безопасности, включенному в сертификат формата X.509;

Отозванные сертификаты – сертификаты, которые не могут больше использоваться для выполнения криптографических или других операций, кроме проверки или подтверждения ранее выполненных. После отзыва сертификата Клиента должен уничтожить секретный ключ, отвечающий этому сертификату;

Блокированные сертификаты – сертификаты, действие которых временно приостановлено и может быть восстановлено через определенное время;

Идентификация – определение, что Клиент есть тот, за которого себя выдает;

Аутентификация – определение, что Пользователь, который зарегистрировался в системе, имеет право доступа к тому или иному объекту системы;

Публикация сертификата – доступ к сертификатам с Веб-сайта УСЦ.