УТВЕРЖДАЮ
Директор Унитарного предприятия
по оказанию услуг
«Удостоверяющий центр «БУТБ»
_____ А.Г. Бобейко
«__11__» _____ 2014г.

Политика применения сертификатов
Удостоверяющего центра системы электронных аукционов
Унитарного предприятия по оказанию услуг «Удостоверяющий центр «БУТБ»

Минск 2014

Содержание

ССЫЛКИ НА НОРМАТИВНЫЕ ДОКУМЕНТЫ

1. Закон Республики Беларусь № 455-З от 10.11.2008 «Об информации, информатизации и защите информации».
2. Закон Республики Беларусь № 113-З от 28.12.2009 «Об электронном документе и электронной цифровой подписи».
3. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 62 от 30.08.2013 «О некоторых вопросах технической и криптографической защиты информации».
4. ГОСТ 21.101-93 Основные требования к рабочей документации.
5. СТБ ISO/IEC 27001-2011 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
6. СТБ 34.101.1-2014 (ISO/IEC 15408-1:2009) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. (ISO/IEC 15408-1:2009, MOD).
7. СТБ 34.101.2-2014 (ISO/IEC 15408-2:2008) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. (ISO/IEC 15408-2:2008, MOD).
8. СТБ 34.101.3-2014 (ISO/IEC 15408-3:2008) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности. (ISO/IEC 15408-3:2008, MOD).
9. СТБ 34.101.17-2012 Информационные технологии. Синтаксис запроса на получение сертификата.
10. СТБ 34.101.19-2012 Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей.
11. СТБ 34.101.48-2012 Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

НКИ	Носитель ключевой информации
ППС	Политика применения сертификатов
СИБ	Система информационной безопасности
СОК	Сертификат открытого ключа
СОС	Список отозванных сертификатов
ТНПА	Технические нормативные правовые акты
УЦ	Удостоверяющий центр
УЦ Биржи	Унитарное предприятие по оказанию услуг «Удостоверяющий центр «БУТБ»
УЦ СЭА	Удостоверяющий центр системы электронных аукционов Унитарного предприятия «УЦ «БУТБ»
ЭЦП	Электронная цифровая подпись

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Абонент – юридическое или физическое лицо, в том числе индивидуальный предприниматель, с которым заключен договор на оказание услуг.

Генерация личного и открытого ключей – процедура, реализующая алгоритм выработки личного ключа и соответствующего ему открытого ключа.

Доверяющая сторона – юридическое или физическое лицо, полагающееся на достоверность сведений, содержащихся в сертификате открытого ключа, и (или) электронную цифровую подпись, проверенную с использованием данного сертификата.

Компрометация личного ключа – утрата доверия к личному ключу.

Носитель ключевой информации – специальное отчуждаемое программно-аппаратное устройство хранения информации, подключаемое к USB-порту ПЭВМ и обеспечивающее хранение личных ключей в зашифрованном виде.

Отзыв сертификата открытого ключа – процедура, заключающаяся в досрочном прекращении действия сертификата открытого ключа.

Политика применения сертификата – установленный набор правил, характеризующих возможность применения сертификатов определенным сообществом субъектов и/или классом приложений с определенными требованиями безопасности.

Приостановление действия сертификата – процедура изменения состояния сертификата открытого ключа с целью исключения использования его на время приостановления.

Регламент УЦ СЭБТ – документ «Регламент работы унитарного предприятия по оказанию услуг «Удостоверяющий центр «БУТБ» по распространению открытых ключей проверки электронной цифровой подписи для участия в биржевой торговле».

Сертификат открытого ключа – электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенным организации или физическому лицу, и иную информацию, предусмотренную Законом Республики Беларусь № 113-З от 28.12.2009 «Об электронном документе и электронной цифровой подписи» и иными актами законодательства Республики Беларусь.

Система информационной безопасности (СИБ) – комплекс организационных и технических мер, направленных на обеспечение безопасности информационных активов, включая разработку и внедрение соответствующих политик и процедур, создание технологической инфраструктуры, внедрение программных и технических средств защиты.

Список отозванных сертификатов – электронный документ, созданный УЦ Биржи и содержащий информацию о сертификатах открытого ключа,

действие которых прекращено или приостановлено до истечения срока действия открытых ключей, указанных в сертификатах открытого ключа.

Срок действия сертификата – промежуток времени, в течение которого Предприятие гарантирует подлинность СОК и актуальность его состояния.

Удостоверяющий центр (УЦ) – поставщик услуг издания, распространения, хранения сертификатов открытых ключей и списков отозванных сертификатов открытых ключей.

Уполномоченный представитель – физическое лицо, наделенное полномочиями на представление интересов юридического или физического лица, в том числе индивидуального предпринимателя, во взаимоотношениях с УЦ Биржи.

ВВЕДЕНИЕ

Политика применения сертификатов (далее – ППС) – это установленный набор правил, характеризующих возможность применения сертификатов определенным сообществом субъектов и/или классом приложений с определенными требованиями безопасности. В ППС основной областью применения требований к управлению жизненным циклом сертификатов открытых ключей (далее – СОК) является Удостоверяющий центр системы электронных аукционов (далее – УЦ СЭА).

Настоящий документ разработан в соответствии с законодательством Республики Беларусь, регулирующим деятельность в области защиты информации, информатизации и электронного документооборота (Законом Республики Беларусь «Об информации, информатизации и защите информации» от 10.11.2008 № 455-З), в том числе с учетом требований СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения СОК удостоверяющих центров» и СТБ ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

ППС разработана в соответствии с документом «Регламент работы унитарного предприятия по оказанию услуг «Удостоверяющий центр «БУТБ» по распространению открытых ключей проверки электронной цифровой подписи для участия в электронных аукционах» (далее – Регламент УЦ СЭА).

УЦ Биржи должен ознакомить абонентов с настоящей ППС.

УЦ Биржи должен уведомлять абонентов и иных заинтересованных лиц о внесении изменений и дополнений в настоящую ППС.

ППС является методологической основой для УЦ Биржи при осуществлении деятельности УЦ СЭА:

- издания и обеспечения жизненного цикла (хранения, приостановления действия, возобновления, отзыв) СОК проверки электронной цифровой подписи для участия в электронных аукционах;
- издания и распространения СОК абонентов;
- издания и хранения списков отозванных СОК абонентов;
- регистрации владельцев личных ключей;
- регистрации заявок на издание и отзыв СОК;
- ведения базы данных изданных СОК абонентов;
- прекращения, приостановления и возобновления действия СОК;
- проверки информации, размещаемой в СОК;
- обеспечения учета и хранения карточек открытых ключей абонентов;
- достоверного подтверждения принадлежности открытого ключа определенной организации или физическому лицу;
- удостоверения формы внешнего представления электронного документа на бумажном носителе.

Требования ППС должны реализоваться УЦ СЭА в соответствии с Регламентом УЦ СЭА.

1 ТРЕБОВАНИЯ К УЧАСТНИКАМ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

1.1 Требования к УЦ СЭА

УЦ СЭА должен выполнять все требования, установленные в данной ППС.

УЦ СЭА несет ответственность в соответствии с законодательством за соответствие процедурам, установленным ППС, даже в случаях выполнения услуг УЦ по распространению открытых ключей субподрядчиками.

Данная ППС не противоречит Регламенту УЦ СЭА.

1.2 Требования к абонентам УЦ СЭА

Абонент УЦ СЭА должен:

- гарантировать, что вся информация, предоставляемая для издания и использования его открытого ключа и СОК, является полной и достоверной;
- использовать личный и открытый ключ только для выработки и поверки электронной цифровой подписи (далее – ЭЦП), а также в соответствии с любыми другими ограничениями, изложенными в Регламенте УЦ СЭА и на сайте УЦ Биржи www.ecp.by.
- осуществлять выработку личного ключа подписи с использованием сертифицированного средства ЭЦП;
- осуществлять выработку открытого ключа на базе личного ключа с использованием сертифицированного средства ЭЦП;
- хранить в тайне личный ключ;
- обеспечивать защиту личного ключа от случайного уничтожения или модификации (изменения);
- отозвать открытый ключ в случае, если тайна соответствующего ему личного ключа нарушена;
- не использовать личный ключ, если соответствующий ему открытый ключ отозван или срок действия такого открытого ключа истек.

В случае если в качестве абонента выступает уполномоченный представитель, то уполномоченный представитель должен информировать абонента о данных требованиях.

1.3 Требования к доверяющей стороне

Перед установлением доверия к электронному документу (в частности, СОК) доверяющие стороны должны:

- убедиться в действительности СОК (включая его проверку на отзыв, приостановку или истечение срока действия);
- удостовериться, что назначение СОК соответствует предполагаемой области применения и любым другим ограничениям, связанным с его использованием, которые указаны в нем или в настоящей ППС.

2 ТРЕБОВАНИЯ К УЦ СЭА

2.1 Требования по управлению ключами

2.1.1 Выработка личного ключа подписи УЦ СЭА

Выработка личного ключа подписи УЦ СЭА должна осуществляться под контролем как минимум двух сотрудников УЦ Биржи в конструктивно защищенной среде.

Выработка личного ключа подписи и открытого ключа проверки подписи УЦ СЭА должна осуществляться с использованием сертифицированного программно-аппаратного средства ЭЦП.

До истечения срока действия личного ключа подписи УЦ СЭА, сотрудники УЦ Биржи должны выработать новую пару ключей для подписи издаваемых СОК и принимать все необходимые меры для того, чтобы избежать нарушения деятельности любого участника, доверяющего СОК УЦ СЭА. Новые ключи УЦ СЭА также должны создаваться и распространяться в соответствии с настоящей ППС.

2.1.2 Хранение, резервное копирование и восстановление личного ключа подписи удостоверяющего центра

Личный ключ подписи УЦ СЭА должен храниться в защищенном виде на носителях ключевой информации (далее – НКИ).

УЦ СЭА должен осуществлять резервное копирование своих личных ключей.

Резервные копии личных ключей должны храниться в защищенном виде на НКИ.

Личные ключи УЦ СЭА должны копироваться и восстанавливаться в присутствии минимум двух сотрудников УЦ Биржи.

Средства контроля доступа к НКИ, на которых хранятся резервные копии личных ключей УЦ, должны гарантировать отсутствие несанкционированного доступа к ним.

2.1.3 Распространение открытых ключей УЦ СЭА

УЦ СЭА должен распространять свой открытый ключ проверки подписи в виде СОК.

Доверяющая сторона должна провести проверку подлинности и целостности открытого ключа ЭЦП УЦ СЭА при его получении.

2.1.4 Депонирование личного ключа УЦ СЭА

УЦ СЭА не должен осуществлять депонирование своих личных ключей.

2.1.5 Использование личного ключа УЦ СЭА

УЦ СЭА должен использовать личные ключи только для издания СОК, списка отозванных сертификатов (далее – СОС) и предоставления информации о статусе СОК.

2.1.6 Окончание срока действия личного ключа УЦ СЭА

Личные ключи подписи УЦ СЭА, по окончании срока их действия, должны не использоваться и уничтожаться без возможности восстановления.

2.1.7 Управление средством ЭЦП, используемым для издания СОК

УЦ СЭА должен обеспечивать безопасность средства ЭЦП в течение всего срока его применения для издания СОК.

УЦ СЭА должен гарантировать, что:

- средство ЭЦП, используемое для издания СОК и СОС, не было повреждено во время поставки;
- средство ЭЦП, используемое для издания СОК и СОС, не было скомпрометировано во время хранения;
- установка, активация, резервное копирование и восстановление ключей ЭЦП УЦ СЭА в средстве ЭЦП проводятся под контролем не менее двух доверенных сотрудников УЦ Биржи;
- средство ЭЦП, используемое для издания СОК или СОС, функционирует правильно.

2.2 Требования по управлению СОК

2.2.1 Регистрация абонента

УЦ СЭА при регистрации абонента для получения СОК должен установить и подтвердить подлинность, полноту и достоверность представленных сведений.

До вступления в договорные отношения абонент должен ознакомиться с нормами и правилами, касающимися использования СОК. УЦ СЭА должен предоставлять данную информацию с использованием долговечных носителей информации, в том числе в электронном виде, на государственном языке Республики Беларусь.

УЦ СЭА в соответствии с законодательством должен проводить проверку подлинности абонента, а так же полноту и достоверность представленных сведений.

Личность физического лица должна проверяться на основании документа, удостоверяющего личность в соответствии с законодательством, при этом должны подтверждаться фамилия, имя и отчество, дата рождения, идентификационный номер.

В случае если абонентом является юридическое лицо, для проверки его подлинности должно быть предоставлено подтверждение следующей информации:

- полного ФИО, даты рождения, идентификационного номера уполномоченного лица;
- полного наименования и правового статуса юридического лица;
- любой соответствующей существующей регистрационной информации о юридическом лице;
- доказательства того, что абонент является уполномоченным представителем юридического лица.

УЦ СЭА должен регистрировать всю информацию, используемую для проверки личности абонента, включая номер документа, удостоверяющего личность в соответствии с законодательством, дату выдачи данного документа, наименование органа, выдавшего его, а также другие данные.

Если регистрационные документы подает не сам абонент, а уполномоченный представитель, то необходимо предоставить в УЦ СЭА подтверждение того, что уполномоченный представитель имеет право осуществлять данную деятельность (т. е. запрос на получение СОК для всех членов указанной организации формирует уполномоченный представитель).

УЦ СЭА должен регистрировать договор с уполномоченным представителем, который включает:

- права и обязанности абонента;
- следующие положения (либо ссылки на документы, в которых регламентированы данные положения):
    - согласие на то, чтобы УЦ СЭА хранил информацию, предоставленную при регистрации, осуществлял любой последующий отзыв и передачу данной информации третьим сторонам на тех же условиях, какие требуются в соответствии с данной ППС в случае прекращения деятельности УЦ СЭА;
    - согласие абонента на опубликование СОК и условия его публикации;
    - подтверждение того, что информация, содержащаяся в СОК, является точной и достоверной.

Указанная выше регистрационная информация должна храниться для предоставления доказательств при судопроизводстве в течение срока, установленного законодательством Республики Беларусь.

Абонент вместе с созданием запроса на издание СОК формирует в УЦ СЭА карточку открытого ключа. На карточке открытого ключа абонента проставляется собственноручная подпись представителя абонента и оттиск печати владельца личного ключа, являющегося организацией, или собственноручная подпись владельца личного ключа, являющегося физическим лицом, в том числе личная подпись индивидуального предпринимателя.

2.2.2 Издание СОК

СОК, издаваемые УЦ СЭА, должны содержать:

- идентификатор УЦ СЭА;

- информацию, однозначно идентифицирующую организацию или физическое лицо, которые являются владельцами открытого ключа;
- назначение использования СОК;
- значение открытого ключа;
- начало и конец срока действия СОК;
- идентификационный номер СОК;
- ЭЦП УЦ СЭА.

УЦ СЭА должен гарантировать уникальность идентификационного номера СОК.

УЦ СЭА должен обеспечивать конфиденциальность и целостность регистрационных данных, передаваемых при обмене с абонентом.

2.2.3 Распространение СОК

УЦ СЭА должен вести реестр изданных СОК в электронном виде или на бумажном носителе в течение установленного срока хранения.

УЦ СЭА должен информировать абонентов и иных заинтересованных лиц о порядке осуществления деятельности по распространению открытых ключей путем размещения соответствующей информации на сайте УЦ Биржи;

УЦ СЭА может выполнять отзыв действующего СОК и выпуск нового СОК в соответствии с п. 2.2.4 и п. 2.2.2.

Информация о назначении СОК должна быть доступна доверяющим сторонам.

Данная информация должна быть доступна 24 часа в сутки 365 дней в году. В случае отказа системы, сервисов или при наличии других факторов, не зависящих от УЦ СЭА, УЦ СЭА должен принять все необходимые меры, чтобы гарантировать, что данная информационная услуга будет недоступна только в течение максимально короткого интервала времени.

2.2.4 Отзыв и приостановка действия СОК

УЦ СЭА должен отзывать СОК на основании заявления и в сроки, установленные в Регламенте УЦ СЭА.

Заявления, связанные с отзывом СОК, должны обрабатываться УЦ СЭА по мере их поступления.

Заявления, связанные с отзывом, должны идентифицироваться и проверяться УЦ СЭА на предмет их получения из достоверных источников.

Абонент отозванного или приостановленного СОК должен информироваться УЦ СЭА об изменении статуса его СОК.

Если СОК отозван, он не должен использоваться в дальнейшем никогда.

Информация о статусе СОК должна распространяться УЦ СЭА посредством издания СОС, который должен быть издан и опубликован в течение 30 минут с момента отзыва СОК.

Услуги УЦ СЭА по управлению отзывом и получению статуса СОК должны быть доступны 24 часа в сутки 365 дней в году. В случае отказа системы,

сервисов или при наличии других факторов, не зависящих от УЦ СЭА, УЦ СЭА должен гарантировать, что данная информационная услуга будет недоступна только в течение максимально короткого интервала времени.

2.2.5 Возобновление действия СОК и обновление данных

Возобновление действия СОК должно осуществляться УЦ СЭА на основании заявления абонента.

Возобновление действия СОК должно осуществляться без изменения открытого ключа абонента и любой другой регистрационной информации, содержащейся в данном СОК.

Перед тем как восстановить СОК УЦ СЭА должен удостовериться, что информация, использованная для подтверждения личности и полномочий абонента, на момент обращения является действительной.

2.3 Управление деятельностью УЦ СЭА

2.3.1 Управление безопасностью

Руководство УЦ СЭА несет ответственность за организацию работ по защите информации, определению политики информационной безопасности УЦ СЭА и за ознакомление с ней всего персонала УЦ СЭА, на который она распространяется.

Требования к информационной безопасности УЦ СЭА должны определяться с помощью систематической оценки рисков. Оценка рисков должна выполняться периодически и методическим способом, чтобы учесть изменения в требованиях защиты и в рисковых ситуациях, например в активах, угрозах, слабых местах, негативных воздействиях, оценке значительности рисков, а также когда происходят значительные изменения.

УЦ СЭА несет ответственность за все аспекты предоставления услуг по распространению открытых ключей, даже если некоторые из этих услуг предоставляются его субподрядчиками. Ответственность третьей стороны определяется соответствующими соглашениями между ними.

УЦ СЭА должен разрабатывать документы по контролю физической безопасности помещений УЦ СЭА и его операционным процедурам для информационных систем и активов, реализующих услуги по распространению открытых ключей.

2.3.2 Распространение нормативных и организационных документов

УЦ СЭА должен гарантировать, что необходимые нормативные и организационные документы УЦ СЭА являются доступными для абонентов и доверяющих сторон.

УЦ СЭА должен предоставлять доступ абонентам к следующим нормативным и организационным документам УЦ СЭА:

- настоящей ППС;
- Регламенту УЦ СЭА;

- документам об ограничениях по использованию издаваемых СОК;
- документам об обязанностях абонента.

2.3.3 Классификация и управление активами

Все активы УЦ СЭА должны быть четко определены, должна быть составлена и должна поддерживаться в рабочем состоянии опись всех важных активов. Кроме того, собственность и классификация информации должны быть согласованы и документально подтверждены для каждого из активов. На основе важности актива должны быть определены его ценность для УЦ СЭА и категория защиты, уровни защиты, соразмерные с важностью активов. Также необходимо идентифицировать владельцев всех основных активов и определить их ответственность за поддержание основных мероприятий по управлению информационной безопасностью.

2.3.4 Вопросы безопасности, связанные с персоналом

УЦ СЭА должен привлекать для реализации своих услуг по распространению открытых ключей персонал, который обладает необходимой квалификацией и опытом и прошел проверку на соответствие кадровой политике УЦ СЭА.

В должностных инструкциях сотрудников УЦ СЭА должны быть определены их роли, права, обязанности и ответственность за обеспечение защиты информации. Также в них должны быть определены права и порядок доступа к защищаемой информации, меры дисциплинарного воздействия, которые будут применимы в случае несанкционированных действий, нарушения политики информационной безопасности или процедур УЦ СЭА.

2.3.5 Физическая защита и защита от воздействий окружающей среды

УЦ СЭА должен обеспечивать физический доступ к оборудованию, используемому для изготовления и отзыва СОК, только уполномоченным лицам.

УЦ СЭА должен осуществлять контроль во избежание утери, повреждения или компрометации ключевой информации, которая может привести к приостановлению его деятельности.

УЦ СЭА должен осуществлять контроль во избежание компрометации или кражи информации и оборудования, используемого для обработки этой информации.

Должен быть создан серверный центр УЦ СЭА для реализации физически защищенной среды, которая обеспечивает обнаружение и предотвращение несанкционированного использования, доступа или разглашения информации, обрабатываемой в УЦ СЭА.

УЦ СЭА должен осуществлять физическую защиту и защиту от воздействий окружающей среды для помещений, в которых расположены системные ресурсы, самих системных ресурсов и оборудования, используемого для поддержания деятельности УЦ СЭА.

2.3.6 Управление операционной деятельностью

Информационная система УЦ СЭА и информация, обрабатываемая в УЦ СЭА, должны быть защищены от вирусов и недоверенного программного обеспечения.

В УЦ СЭА должны протоколироваться и применяться меры быстрого реагирования на все сбои и инциденты в работе СИБ.

В УЦ СЭА должны быть определены и реализованы процедуры, влияющие на предоставление услуг по распространению открытых ключей.

В УЦ СЭА должно проводиться планирование мероприятий по обеспечению достаточности системных ресурсов и дискового пространства с целью обеспечения надлежащей обработки и хранения информации.

УЦ СЭА должен своевременно и скоординировано принимать меры по быстрому реагированию на инциденты в области безопасности и ограничению влияния нарушений безопасности.

В УЦ СЭА журналы аудита должны регулярно контролироваться на предмет наличия следов вредоносной деятельности.

2.3.7 Управление системным доступом

При подключении информационной системы УЦ СЭА к глобальной сети Интернет, должны применяться средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь.

В СИБ УЦ СЭА могут применяться средства криптографической защиты информации для обеспечения конфиденциальности, контроля целостности (неизменности) и подлинности информации.

УЦ СЭА должен ограничивать доступ к информации и системные функции приложений УЦ СЭА в соответствии с Политикой ИБ, а также должен обеспечивать достаточный контроль компьютерной безопасности для разделения администраторов безопасности и прочих сотрудников УЦ СЭА. Должен предоставляться доступ только к тем ресурсам, которые необходимы для осуществления деятельности в качестве пользователя.

Сотрудники УЦ СЭА должны успешно пройти процедуру идентификации и аутентификации перед пользованием критически важным оборудованием, связанным с управлением СОК.

Сотрудники УЦ СЭА должны нести ответственность за свои действия, например, путем сохранения записей событий.

УЦ СЭА должен гарантировать, что локальные сетевые компоненты содержатся в физически безопасном окружении и что их конфигурация периодически проверяется на соответствие требованиям, установленным в Политике ИБ.

В серверном центре УЦ СЭА организовано постоянное наблюдение и установлены средства оповещения о тревоге, чтобы иметь возможность соответствующим образом обнаруживать, регистрировать и реагировать на несанкционированные и ошибочные попытки доступа к его ресурсам.

Приложение, определяющее статус отзыва, должно осуществлять контроль доступа на предмет попыток изменения информации о статусе отзыва.

2.3.8 Внедрение и обслуживание информационных систем

УЦ СЭА должен использовать безопасные доверенные информационные системы и продукты, которые защищены от модификации.

Анализ требований безопасности должен проводиться на всех этапах разработки информационных систем для УЦ СЭА с такой степенью детализации, чтобы обеспечить необходимый уровень гарантии того, что в них надежно реализованы механизмы безопасности.

2.3.9 Восстановление при сбоях и обеспечение непрерывности деятельности

УЦ СЭА должен гарантировать, что в случае сбоя, включая компрометацию личного ключа подписи УЦ СЭА, действия возобновляются настолько быстро, насколько это возможно.

УЦ СЭА должен иметь план восстановления при сбоях и обеспечения непрерывности деятельности, содержащий описание всех разумно предсказуемых типов сбоев и компрометаций, влияющих на оказание услуг по распространению открытых ключей.

Данные информационных систем УЦ СЭА, необходимые для продолжения деятельности УЦ СЭА, должны подвергаться резервному копированию и храниться в безопасных местах, пригодных для того, чтобы УЦ СЭА мог оперативно возобновить деятельность в случае аварии или сбоя.

План восстановления при сбоях и обеспечения непрерывности деятельности УЦ СЭА должен рассматривать компрометацию или подозрение на компрометацию личного ключа подписи УЦ СЭА как сбой.

В случае компрометации личного ключа подписи УЦ СЭА он должен выполнить следующие обязательства:

- проинформировать всех абонентов, доверяющие стороны и другие УЦ, с которыми он заключил договоры или другие формы соглашений, о компрометации;
- объявить о том, что все СОК и СОС, изданные с использованием данного ключа УЦ СЭА более не являются действительными.

2.3.10 Прекращение функционирования УЦ СЭА

В случае прекращения функционирования УЦ СЭА, он должен гарантировать, что потенциальные угрозы для абонентов и доверяющих сторон сведены к минимуму, а также информация о СОК будет сохранена для предоставления в суд в случае необходимости.

В случае прекращения функционирования УЦ СЭА должен:

- проинформировать абонентов, доверяющие стороны и другие УЦ, с которыми он заключил договоры или другие формы соглашений;

- ограничить все полномочия субподрядчиков, которые оказывают услуги по распространению открытых ключей в интересах УЦ СЭА;
- осуществить необходимые процедуры по передаче обязанностей для хранения регистрационной информации и записей архивов, включая информацию о статусе отзыва, на соответствующий период времени, оговоренный с абонентами и доверяющими сторонами;
- уничтожить свои личные ключи подписи.

2.3.11 Сохранение информации, касающейся СОК

УЦ СЭА должен гарантировать, что вся соответствующая информация, относящаяся к СОК, сохраняется на установленный срок, в частности с целью ее предоставления в суд по искам к электронным документам.

УЦ СЭА должен поддерживать конфиденциальность и целостность текущих и архивированных записей, касающихся СОК.

УЦ СЭА должен предоставить доступ к записям, касающимся СОК, в целях представления их в суд.

События и данные, которые должны регистрироваться, должны документироваться УЦ СЭА.

УЦ СЭА должен гарантировать, что будут регистрироваться все события, связанные с регистрацией абонентов и выпуском СОК.

УЦ СЭА должен сохранять всю регистрационную информацию, включая:

- номер документа заявителя, удостоверяющего его личность в соответствии с законодательством, дату выдачи данного документа, наименование органа, выдавшего его, идентификационный номер;
- копии заявлений и документов, удостоверяющих личность, включая подписанный договор;
- все дополнительные материалы к абонентскому договору;
- идентификатор организации, принимающей заявления.

2.4 Организационные положения

Принципы и правила деятельности УЦ СЭА должны обеспечивать условия для независимой деятельности УЦ СЭА и объективности принимаемых им решений.

УЦ Биржи зарегистрирован в качестве юридического лица в соответствии с законодательством.

УЦ Биржи обеспечивает оказание услуг любым лицам и организациям, заинтересованным в получении услуг УЦ СЭА и обратившимся в УЦ Биржи за такими услугами.

Ответственность УЦ Биржи предусматривается в договоре, заключаемом УЦ Биржи с лицом или организацией, которым оказываются соответствующие услуги.

В УЦ Биржи должен быть установлен порядок рассмотрения обращений и жалоб, поступающих от потребителей услуг УЦ СЭА, а также порядок разрешения споров, возникающих в связи с оказанием услуг УЦ СЭА.

Деятельность УЦ Биржи не должна зависеть от действий и решений сторонних организаций, в том числе в принятии решений о предоставлении услуг, порядке и приостановлении их оказания.

ПРИЛОЖЕНИЕ

к документу «Политика применения сертификатов» СИБ УЦ СЭА

Пример карточки открытого ключа

КАРТОЧКА ОТКРЫТОГО КЛЮЧА

Наименование организации владельца открытого ключа: *Общество с ограниченной ответственностью "Славтехнология"*
Ф.И.О.: *Сенюк Владимир Вячеславович*
Страна: *BY*
Область: *Минская область*
Населенный пункт: *п.о. Озерцо*
Должность: *экономист*
Данные из документа, удостоверяющего личность: *Паспорт MP 2965660, личный ¹ 3290661A015PB3, выдан: Московским РУВД г. Минска 2011-04-21*
Адрес: *223021, Минская область, Минский р-н, п.о. Озерцо, Менковский тракт, 1, 12*
Краткое наименование организации: *Славтехнология, ООО*
Адрес электронной почты: *Slavt@mail.ru*
УНП организации: *190267765*
Уникальный идентификатор: *UNP=190267765/OKPO=37533317/EGR=190267765*

Использование ключа:
Согласование ключа, Шифрование данных, Шифрование ключа, Цифровая подпись
Назначение ключа:
Использование на электронных площадках отобранных для проведения аукционов в электронной
форме(1.2.643.6.3.1.1)
Юридическое лицо(1.2.643.6.3.1.2.1)
Участник размещения заказа(1.2.643.6.3.1.3.1)
Администратор организации(1.2.643.6.3.1.4.1)
Уполномоченный специалист(1.2.643.6.3.1.4.2)
Специалист с правом подписи контракта(1.2.643.6.3.1.4.3)
Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
Защищенная электронная почта(1.3.6.1.5.5.7.3.4)

Дополнительные атрибуты ключа:
Идентификатор открытого ключа (2.5.29.14): 7543 7015 6FFE CA62 EF05 ED2F 666B 4402 B5ED
6334

Срок использования личного ключа: определяется сроком действия сертификата.
Срок действия открытого ключа: определяется сроком действия сертификата.
Алгоритм: *СТБ 1176.2-99 / РД РБ DH*
Значение открытого ключа:
30820124 30818F06 092B0601 0401E270 01230381 81029F02 5FDC8E9C 4724FF59 EB89C23C 5DADF183
34D034E0 6A22EF98 4FA4B6CE EAE925B4 8BA4E866 7F91A639 3DA913E3 DD43BDAD 5A2D41AD DC5A7099
B63242F0 B46DF47A B53F6131 7CA7700F E06068E3 EBB5F5D4 376C1A98 9463FA21 82ED5A4B 27150583
CDC09168 321AEA16 43C55982 59D01DCA D3141E3D E2C4D109 3A8C27B8 4B4C3081 8F06092B 06010401
E2700120 03818102 87BF0734 3A86EBBA A8175BFA 74222020 45FEBDF5 911C1657 435C3A72 AB28ACE4
611366DB 9F05C213 EE5D62A9 C2B29C3D B3350925 4337C1C4 D4F17BC4 9190219C 90528246 2FFFC476
43F7FD9F D0121859 33CAFE0D 5E9CEE71 380FB185 13E2AEC0 73670169 EB890CFF 9D4CD288 28DF2753
A5150DB2 B5DB6724 5DF97CE0 2BC68690
(DER-представление ASN.1)
Параметры алгоритма:
идентификатор объекта согласно РД НБ РБ 07040.1206-2004

1.3.6.1.4.1.12656.7.2

Подпись владельца открытого ключа:

_____

_____
_____

Карточка удостоверена:

_____

_____
_____

М.П.