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

Политика применения сертификатов
Удостоверяющего центра системы электронных биржевых торгов
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 СЭБТ	Удостоверяющий центр системы электронных биржевых торгов 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 абонентов 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 биржевых торгов (далее – УЦ СЭБТ).

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 биржевой торговле» (далее – Регламент УЦ СЭБТ).

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 СЭБТ:

- издания и обеспечения жизненного цикла (хранения, приостановления действия, возобновления, отзыв) СОК проверки электронной цифровой подписи для участия в биржевой торговле;
- 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 СЭБТ в соответствии с Регламентом УЦ СЭБТ.

1 ТРЕБОВАНИЯ К УЧАСТНИКАМ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

1.1 Требования к УЦ СЭБТ

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

УЦ СЭБТ 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 СЭБТ.

1.2 Требования к абонентам УЦ СЭБТ

Абонент УЦ СЭБТ 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 СЭБТ 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 СЭБТ

2.1 Требования по управлению ключами

2.1.1 Выработка личного ключа подписи УЦ СЭБТ

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

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

До истечения срока действия личного ключа подписи УЦ СЭБТ, 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 СЭБТ. Новые ключи УЦ СЭБТ 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 СЭБТ должен храниться в защищенном криптографическими методами файловом контейнере на сервере УЦ СЭБТ.

УЦ СЭБТ должен осуществлять резервное копирование своих личных ключей.

Резервные копии личных ключей должны храниться в защищенном виде на носителях ключевой информации (далее – НКИ).

Личные ключи УЦ СЭБТ 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 СЭБТ

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

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

2.1.4 Депонирование личного ключа УЦ СЭБТ

УЦ СЭБТ не должен осуществлять депонирование своих личных ключей.

2.1.5 Использование личного ключа УЦ СЭБТ

УЦ СЭБТ 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 СЭБТ

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

2.1.7 Управление средством ЭЦП, используемым для издания СОК

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

УЦ СЭБТ 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 СЭБТ 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 СЭБТ 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 СЭБТ должен предоставлять данную информацию с использованием долговечных носителей информации, в том числе в электронном виде, на государственном языке Республики Беларусь.

УЦ СЭБТ 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 СЭБТ 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 СЭБТ 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 СЭБТ 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 СЭБТ 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 СЭБТ;
    - 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 запросом на издание СОК должен предоставить в УЦ СЭБТ карточку открытого ключа, на которой проставлена 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 СЭБТ, должны содержать:

- идентификатор УЦ СЭБТ;
- 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 СЭБТ.

УЦ СЭБТ должен гарантировать уникальность идентификационного номера СОК.

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

2.2.3 Распространение СОК

Сертификат открытого ключа абонента УЦ СЭБТ, после своего издания, становится действительным. УЦ СЭБТ должен известить абонента об издании его СОК. УЦ СЭБТ должен поместить изданный СОК на сервер реестра сертификатов УЦ Биржи.

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

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

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

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

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

Информация о статусе СОК должна распространяться УЦ СЭБТ посредством издания СОС, который должен быть издан и опубликован в течение дня.

Услуги УЦ СЭБТ 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 СЭБТ, УЦ СЭБТ 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 СЭБТ 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 СЭБТ должен удостовериться, что информация, использованная для подтверждения личности и полномочий абонента, на момент обращения является действительной.

2.3 Управление деятельностью УЦ СЭБТ

2.3.1 Управление безопасностью

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

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

2.3.2 Распространение нормативных и организационных документов

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

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

- настоящей ППС;
- Регламенту УЦ СЭБТ;
- документам об ограничениях по использованию издаваемых СОК;
- документам об обязанностях абонента.

2.3.3 Классификация и управление активами

Все активы УЦ СЭБТ 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 СЭБТ 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 СЭБТ 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 СЭБТ.

В должностных инструкциях сотрудников УЦ СЭБТ 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 СЭБТ.

2.3.5 Физическая защита и защита от воздействий окружающей среды

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

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

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

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

УЦ СЭБТ 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 СЭБТ.

2.3.6 Управление операционной деятельностью

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

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

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

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

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

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

2.3.7 Управление системным доступом

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

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

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

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

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

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

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

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

В случае компрометации личного ключа подписи УЦ СЭБТ 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 СЭБТ более не являются действительными.

2.3.10 Прекращение функционирования УЦ СЭБТ

В случае прекращения функционирования УЦ СЭБТ, 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 СЭБТ 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 СЭБТ;
- 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 СЭБТ 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 СЭБТ должен поддерживать конфиденциальность и целостность текущих и архивированных записей, касающихся СОК.

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

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

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

УЦ СЭБТ 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 СЭБТ должны обеспечивать условия для независимой деятельности УЦ СЭБТ 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 СЭБТ 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 СЭБТ, а также порядок разрешения споров, возникающих в связи с оказанием услуг УЦ СЭБТ.

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 СЭБТ

Пример карточки открытого ключа

КАРТОЧКА ОТКРЫТОГО КЛЮЧА

проверки ЭЦП, всего на двух листах

Наименование организации владельца открытого ключа:
Открытое акционерное общество "Белорусская универсальная товарная биржа"
УНП организации: 190542044
ФИО: Дорошко Наталья Евгеньевна
Номер сотового телефона: 375173093733
Юридический адрес
Страна: BY
Область:
Район:
Населенный пункт: г. Минск
Почтовый индекс: 220099
Улица, дом, корпус, офис: ул. Казинца дом 2 квартира/офис 200
Документ, удостоверяющий личность:
паспорт МС1117328 выдан 11.02.2013 Несвижским РОВД Минской области
Идентификационный номер: 4173388B066PB0
Полномочия:
Наименование документа: Доверенность
Номер документа: 16
Дата документа: 01.10.2014
Начало срока полномочий: 01.10.2014
Окончание срока полномочий по: 30.09.2017
Срок действия открытого ключа:
Начало: 2014-10-02T12:27:46Z
Окончание: задано сроком действия сертификата
Срок использования личного ключа подписи:
Начало: 2014-10-02T12:27:46Z
Окончание: задано сроком действия сертификата
Дополнительные атрибуты ключа:

Подпись и удостоверение первого листа карточки открытого ключа

Подпись владельца открытого ключа
_____ Дорошко Наталья Евгеньевна
" ___ " _____ 20 г.
М.П.

Карточка удостоверена:
_____ **(** _____ **)**
" ___ " _____ 20 г.
М.П.

Алгоритм: СТБ 1176.2-99

Значение открытого ключа (*число в шестнадцатеричной системе счисления***):**

1358bad5 433bf9ef 86927d42 485b0eb8 b1e83d3c d67a9a27 f390fed4 3c82d689
c131abf1 fbd6ea2a 4f12c834 a6115851 105841b1 7cb4bbc4 3124441c b30adb5c
f2b099fa 334a2b2f f27eb320 07f5a8b5 93c54c50 338310a4 4ce64526 223aafb1
097f6f76 66d5b764 e738b6f7 80be8801 a64cc31e e31c0526 2da0e13d 3c1811d8

Параметры алгоритма:

Параметр **L:** 1022

Параметр **R:** 175

Параметр **P** (*число в шестнадцатеричной системе счисления*):

3da3010d 54526f24 0ccd388c df02ae5d b229f35b 87bebfdb 2e23750c 89bd46e7
5a6796af a758232b 55f4c26b 19c9f084 682384de 78d1b226 d37a354a 7437adcb
b2320c6e 270503fa da9d59d7 ce79aa8f 11a3f6bc c12da658 ab567cf7 8f2a7054
f1ead0f7 394d396f 6ca2d0ae 85a85176 ec5a5416 d2914435 e450cb5b b9088809

Параметр **Q** (*число в шестнадцатеричной системе счисления*):

000050f8 859794d5 acf186c8 f7502c2d 46e4966a 14a723e1

Параметр **A** (*число в шестнадцатеричной системе счисления*):

01ac6065 d853fcf6 78aeb339 8d35664a 220359d8 5b26741a 7ea9ff69 1bf229cc
82e1300e c1d011ce 168ac2c0 3304c628 57be6a5d 4ce3d795 97363e03 8e9f9c5f
e3a1b02e 818b4e0f 0b885203 ea9f7777 a8a243e3 bb5e81e5 b648ad65 08a9b757
5701506b a5687af3 695426b1 c368b8e5 51cc8876 d4766d16 1e238382 7758662b

Параметр **H** (*последовательность байтов в шестнадцатеричной системе счисления*):

88E3F4FBA32FF8CF2A3E9847516C1A4968C855CD30314874839D32E295DE8AF9

Последовательность целых чисел $\mathbf{d_0, d_1,..., d_t}$: 513, 257, 129, 65, 33, 17.

Последовательность целых чисел $\mathbf{r_0, r_1,..., r_s}$: 175, 91, 49, 28, 17.

Последовательность чисел $\mathbf{z_1, z_2,..., z_{31}}$(*в шестнадцатеричной системе счисления*):

0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001,
0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001, 0001,
0001, 0001, 0001, 0001, 0001, 0001, 0001.

Параметр **D** для генерации параметра **A** (*число в шестнадцатеричной системе счисления*):

209f1a68 be785508 4431f58d be108055 f7ecf469 c3f51753 f6cf0794 eb73a89e
08ac0fe3 60467f1b 2b60d9d7 cd828852 4c5c55bb ea8b16d2 75fa3186 4ceacc10
1281ac66 4321ad1f f8ff7d12 4cec2b65 b052370d e07627c0 a94a2cd7 8e341a40
cf7e66ab d01c64af 010dc3f9 99b22bcf 2b174845 28d0a081 cbac41a3 f41fb001

Подпись владельца открытого ключа

_____ Дорошко Наталья Евгеньевна

" ___ " _____ 20 г.

М.П.

Карточка удостоверена:

_____ **(** _____ **)**

" ___ " _____ 20 г.

М.П.