Асланов Ильгар Исмет оглы
канд. физ.-мат. наук, доцент
Гасанова Севиндж Эльдар гызы
канд. физ.-мат. наук, ассистент
Азербайджанский медицинский университет
г. Баку, Азербайджанская Республика

DOI 10.21661/r-553273

ИСПОЛЬЗОВАНИЕ СЕРТИФИКАТОВ ЭЦП СТАНДАРТА X.509 В КОРПОРАТИВНЫХ ТОРГОВО-РАСЧЕТНЫХ СИСТЕМАХ

Аннотация*: в статье рассмотрен проект и реализация аппаратной и программной платформы биржевой системы торгов. Описана кластерная инфраструктура и клиентское программное обеспечение комплекса. Показан и обоснован выбранный протокол в целях защиты целостности и безопасной передачи данных.*

Ключевые слова*: комплекс, программное обеспечение, стандарт, аутентификация.*

Современные информационные технологии, внедряемые в корпоративной биржевой среде призваны реализовать несколько ключевых задач – от полной аппаратной замены всего Торгово-Расчетного комплекса и смены ее программной платформы (переход на другую СУБД и ОС) до получения улучшенной программной оболочки для ведения биржевых операций.

На стадии проектирования Торгово-Расчетной Системы в системе BEST (Биржевая Электронная Система Торгов) на Бакинской Бирже (АОЗТ «BBVB») были проведены соответствующие работы для получения однородного программно-аппаратного комплекса с использованием передовых достижений в этих областях. Для реализации этого проекта была предварительно подготовлена вся инфраструктура на BBVB, был принят свод правил с учетом требований ISO и собран в отдельном документе по ИТ-безопасности с обязательным исполнением всеми участниками торгов.

Свою реализацию Система получила на Серверах HP rx2620 на базе процессоров с архитектурой Intel Itanium, а для хранения файлов базы данных используется дисковый массив с 4-мя носителями. Два Сервера объединены в Кластер – софтовый, RAID 0. Для построения кластера используется HP ServiceGuard. На кластере работают два пакета: Торговой Системы и Расчетной Системы. Пакеты работают на разных узлах. Серверная часть работает под управлением 64-х разрядной ОС HP Unix. Клиентская часть разработана для платформ Windows 7 и выше с приложением, созданным на языке C++.

Доступ к Торговой базе осуществляется при помощи клиентского программного обеспечения через Сервер Приложений. При его создании разработчиком ПО использовались технологии Java и CORBA. Учитывая то, что большинство клиентов подключаются к ресурсам BBVB при помощи Удаленных Рабочих Мест посредством Интернета, Система безопасности дополнена средствами шифрования и дешифрования данных и средствами формирования и проверки электронно-цифровой подписи (ЭЦП), что на сегодняшний день является наиболее надежной защитой целостности данных. Здесь выбор сделан в пользу международного стандарта X.509, использующего криптографический протокол, обеспечивающий безопасную передачу данных по сети Интернет – SSL, т.е. все соединения клиентских мест с сервером приложений шифруются при помощи этого протокола защищённых сокетов. Вход в Систему в окне интерфейса осуществляется только после ввода ключевой фразы.

Для доступа в Системе с Удаленных Рабочих Мест использованы сертификаты Microsoft Root Certificate Authority, поддерживающие другие известные удостоверяющие центры (такие как VeriSign, Thawte и др.). Сертификаты выдаются внутрибиржевым Удостоверяющим Центром, генерируемые в режиме оффлайн на Сервере Аутентификации, находящийся вне локальной Сети Биржи. Биржевой сервер генерирует запрос и отправляет его пользователю А. Пользователь А шифрует запрос при помощи ключа, который хранится на сервере. Сервер шифрует и сравнивает с шифровым текстом пользователя А. При их совпадении, аутентификация проходит успешно (рис. 1).

Рис. 1. Аутентификация по схеме «запрос-ответ».

Здесь использованы стандарты, рекомендуемые в постановлениях Кабинета Министров Азербайджанской Республики по таким критериям, как алгоритм RSA с длиной ключа от 1024 бит, хэш-функция и др. [1; 2]. Доступ же уполномоченных лиц к Расчетной Системе осуществляется при помощи клиентского интерфейса путем прямого соединения с базой данных.

При создании Системы на BBVB за основу брали технические и программные средства с критериями повышенной надежности и отказоустойчивости. Таким образом, удалось обеспечить полную аппаратную и программную совместимость используемых средств и создать Биржевую Торгово-Расчетную Система с гибким инструментарием и привлечением большего количества пользователей системы BEST. Этот опыт может быть полезен при построении Торговых Систем бирж и в странах СНГ [3].

В итоге, данное сочетание аппаратных и программных средств обеспечило увеличение производительности системы, ее безопасность и надежность.

Список литературы

1. Постановление Кабинета Министров Азербайджанской Республики №27 от 28 Января 2006 г.

2. Постановление Кабинета Министров Азербайджанской Республики №6 от 16 Января 2008 г.

3. Международная ассоциация Бирж стран СНГ [Электронный ресурс]/ – Режим доступа: http://mab.micex.ru