

Ключи к успеху

Технические и программные средства IBM стали основой для создания защищенной системы электронной почты в российском «БТА Банке»

«БТА Банк» (до июня 2008 года — «СлавинвестБанк») — универсальный банк, входящий в сотню крупнейших банков России, преследует амбициозную цель предложить рынку лучшие банковские продукты и стандарты обслуживания, развивая современные технологии и процессы корпоративного управления.

В рамках стратегической задачи совершенствования процессов корпоративного управления «БТА Банку» потребовалось создать защищенную систему электронной почты.

Значение электронной почты как одного из каналов передачи управленческой информации трудно переоценить. Однако этот канал становится весьма уязвимым при отсутствии надлежащей защиты. Традиционные протоколы обмена электронной почтой не предусматривают защиты информации от перехвата либо искажения. Эти угрозы актуальны даже для корпоративной сети, не говоря уже о сетях передачи данных общего пользования, к услугам которых неизбежно вынуждены прибегать территориально-распределенные организации. Поэтому информацию, передаваемую по таким сетям, надо защищать: от перехвата с помощью шифрования и от искажения с помощью электронной подписи.

«Поскольку при отправлении сообщений, содержащих конфиденциальную информацию, по открытым сетям не обеспечивалась защита от перехвата и искажения, банк использовал такие средства связи, как обычная почта и курьерская доставка, значительно уступающие в скорости, надежности и удобстве применения электронной почте, — рассказывает Сергей Степун, руководитель банковского сектора Концерна информационных технологий, которому было поручено создание системы. — Безусловно, это отрицательно сказывалось на эффективности управления».

«БТА Банком» была выбрана система криптографической защиты на основе инфраструктуры открытых ключей.

Принцип открытых ключей подразумевает наличие для шифрования и расшифрования сообщения двух различных ключей: открытого и секретного. Ключи связаны между собой так, что сообщение, зашифрованное с помощью доступного отправителю открытого ключа, получатель может расшифровать лишь с помощью секретного ключа. Что касается электронной цифровой подписи, то она генерируется с помощью закрытого ключа и проверяется с помощью открытого. Схемы шифрования с открытым ключом



БТА БАНК

получили широкое распространение в различных протоколах передачи данных, в том числе в системах электронной почты. Инфраструктура открытых ключей определяет политику выпуска цифровых сертификатов, подтверждающих принадлежность открытых ключей их владельцам.

Выбирая систему электронной почты, «БТА Банк» остановился на IBM Lotus Domino/Notes. Преимуществами данного программного обеспечения являются кроссплатформенность, широкие возможности репликации, возможность быстрой разработки и развертывания приложений, а также автономного выполнения приложений на клиентских машинах. Кроме того, криптофункции с использованием открытых ключей являются базовыми сервисами ядра Lotus Notes. Механизмом реализации криптофункций стала система шифрования электронной почты «Шифр ПС», разработанная Концерном информационных технологий.



Система «Шифр ПС»

Система «Шифр ПС» позволяет автоматизировать процесс обработки и передачи конфиденциальной информации по открытым каналам с использованием открытого ключа и принципов криптографии как основного метода обеспечения безопасности в соответствии со стандартами шифрования ГОСТ. В качестве основных компонентов, обеспечивающих шифрование данных, используются средства криптозащиты информации (СКЗИ «Крипто Про»), сертифицированные ФСБ. Система состоит из трех подсистем: подсистемы обработки почтовых сообщений, подсистемы хранения пользовательских сертификатов и подсистемы сбора статистики работы системы. Она представляет собой законченное программное решение и имеет простой и удобный пользовательский интерфейс.

Система обеспечивает выполнение следующих задач:

■ **Шифрование и расшифрование почтовых сообщений.** При этом осуществляется выбор сертификатов в соответствии с адресатами из базы сертификатов, автоматическое шифрование исходящих почтовых сообщений, автоматическое расширение зашифрованных почтовых сообщений при их открытии. Предусмотрена также возможность шифрования/расшифрования группы сообщений по выбору пользователя.

■ **Установка и проверка электронно-цифровой подписи почтовых сообщений.** На исходящие почтовые сообщения электронно-цифровая подпись устанавливается автоматически в соответствии с сертификатом, назначенным конкретному пользователю. При открытии почтового сообщения, содержащего подпись, проверка ЭЦП осуществляется автоматически. Как и в случае шифрования и расшифрования, предусмотрена возможность обработки группы документов.

■ **Настройка параметров шифрования.** Эта группа функций включает в себя настройку типа шифрования при автоматической обработке исходящих почтовых сообщений, задание путей к базам данных сертификатов и статистики, а также настройку автоматической обработки зашифрованных почтовых сообщений.

■ **Работа с сертификатами.** Она предусматривает: ведение списка корневых сертификатов и списка отозванных сертификатов, просмотр сертификатов пользователей в базе данных сертификатов; загрузку сертификата пользователя в ба-

Техническое обеспечение проекта

Картина системы была бы неполной без информации о ее аппаратной части. Важным звеном качественно работающей почтовой системы должны были стать высокопроизводительные серверы. Известно, что лучше всего сочетаются друг с другом технические и программные средства одного и того же производителя. Стандартизация дает определенную свободу в выборе поставщиков, однако экспертиза и проприетарные технологии, повышающие согласованность и надежность совместной работы оборудования и программного обеспечения, зачастую заставляют заказчиков отдавать предпочтение именно им. В качестве технической платформы для системы электронной почты были выбраны серверы IBM eServer xSeries 345.

eServer xSeries 345 — это двухпроцессорные серверы высотой 2U, оснащаемые процессорами Intel Xeon с тактовой частотой до 3,2 ГГц. В сочетании с тактовой частотой системной шины 533 МГц такой показатель обеспечивает превосходную производительность. Максимальная емкость оперативной памяти этих серверов составляет 8 Гбайт; оперативная память обеспечивает обнаружение и коррекцию ошибок по фирменной технологии Chipkill; для установки плат расширения предусмотрены пять разъемов PCI (в том числе четыре PCI-X); в сервер может устанавливаться до шести жестких дисков. Система обладает высокой готовностью благодаря возможности заменять вентиляторы, жесткие диски и источники питания без остановки работы. Для повышения сохранности данных на диске в сервере используется контроллер Ultra320 SCSI с возможностью организации массивов RAID 1. Встроенный процессор системного управления обеспечивает возможность круглосуточного удаленного управления и контроля, генерируя уведомления администраторов о случившихся и возможных неполадках.

зу данных сертификатов из системного хранилища, ключевого контейнера или файла; удаление существующего сертификата пользователя из базы данных; генерацию запроса и получение сертификата пользователя.

Компетенции Концерна информационных технологий по предоставлению услуг в области криптографической защиты подтверждены лицензиями Федеральной службы безопасности РФ.

Результаты и перспективы

Внедрение системы «Шифр ПС» в центральном офисе банка было осу-

ществлено в 2007 году. После установки и настройки программного обеспечения специалисты банка, при консультативной поддержке Концерна информационных технологий, провели испытания системы. Положительные результаты, полученные в ходе тестирования, позволили ввести систему в промышленную эксплуатацию.

«В результате реализации проекта был автоматизирован процесс защиты передаваемой информации, повышена безопасность корпоративной почтовой системы», — констатирует Сергей Степыгин. Он подчеркивает, что внедрение защищенной почтовой системы не привело к усложнению пользовательского интерфейса: «При отправке сообщений система самостоятельно определяет сертификат получателя, шифрует документ и проставляет электронно-цифровую подпись. Сотрудники банка пользуются системой для передачи закрытой информации в автоматическом режиме».

«Использование электронной цифровой подписи позволяет точно определять авторство почтового документа, дает гарантии его подлинности и повышает ответственность сотрудников банка», — добавляет начальник удостоверяющего центра «БТА Банка» Сергей Крапивин. По его словам, в планах банка — дальнейшее внедрение системы «Шифр ПС» в прикладные системы документооборота.

В ближайшее время новую систему электронной почты ожидает своего рода «проверка на прочность». В соответствии с программой стратегического ребрендинга (об этом уже говорилось в самом начале) предусматривается переход банка и его ключевых партнеров под единый бренд БТА, центром которого является акционерное общество «БТА Банк», базирующееся в Казахстане. Перспективный план развития БТА до 2015 года предусматривает выход на ключевые позиции в регионе СНГ и завоевание в России не менее 2% рынка банковских услуг. А в текущем году предполагается открытие в Москве и Санкт-Петербурге не менее 50 отделений. Столь значительное расширение позволит проверить на практике потенциал масштабируемости почтовой системы, а объединение с зарубежным банком станет вызовом для ИТ-службы в части программно-технической и организационной интеграции информационных систем. ✖