ЗАЩИТА ДАННЫХ И KERBEROS

#7 2002
www.win2000mag.ru

Windows® 2000 MAGAZINE/RE

БЕЗОПАСНОСТЬ

ISSN 1563-101X
9 771563 101008 >
00

Безопасность Internet-транзакций в электронном бизнесе

Система безопасности акционерного банка «ИБГ НИКойл»

В.Н. Ануфриев, *заместитель начальника службы внутреннего контроля и управления рисками АБ «Инвестиционно-банковская группа НИКойл»*

И.Н. Калинсков, *главный специалист Специального управления АБ «Инвестиционно-банковская группа НИКойл»*

Финансовая корпорация «НИКойл» реализовала систему безопасности Internet-транзакций в приложениях front-office, включающих систему удаленного управления клиентскими счетами, удаленного получения отчетов о факторинговых операциях, документооборота на электронных торговых площадках и ряд других приложений. В качестве корпоративного стандарта было выбрано решение ООО «КриптоПро», реализующее российские алгоритмы шифрования и использующее криптографический интерфейс компании Microsoft — Cryptographic Service Provider (CSP), а в качестве платформы шлюза безопасности выбран Microsoft Internet Security & Acceleration Server Enterprise Edition.

Требования к системе безопасности акционерного банка «ИБГ НИКойл»

Развитие электронного бизнеса немыслимо без наличия совершенных систем безопасности, включающих надежные средства авторизации, аутентификации и защиты от несанкционированного доступа. Как один из лидеров российского рынка услуг, связанных с электронной коммерцией, компания «НИКойл» была озабочена вопросами безопасности при эксплуатации Internet-приложений и обеспечения безопасности Internet-транзакций клиентов как при проектировании новых систем электронного бизнеса, так и при расширении функциональных возможностей уже имеющихся систем.

Именно поэтому в конце 90-х годов в корпорации была разработана концепция построения системы безопасности приложений front-office, включающих систему удаленного управления клиентскими счетами «Банк-Клиент», систему удаленного управления клиентскими счетами для частных лиц «Internet-Банк», систему удаленного получения отчетов о факторинговых операциях «E-Factoring», систему поддержки удаленного торгового терминала ММВБ «E-trading», систему электронного документооборота на электронных торговых площадках, электронную систему продаж паев инвестиционных фондов, систему удаленного управления счетами-депо «E-depo». При этом к системе безопасности предъявлялись такие требования, как ведение общей клиентской базы в системе безопасности, возможность однократной регистрации клиента в системе безопасности с правом последующего доступа ко всем приложениям, наличие у клиента единого секретного криптографического ключа для работы со всеми приложениями front-office, а также наличие единых, юридически корректных процедур для разбора конфликтных ситуаций, обеспечивающих невозможность оспаривания клиентом основания проведения сделки.

С точки зрения функциональности система безопасности должна была обеспечивать двустороннюю аутентификацию клиентов и серверов приложений и защиту трафика клиента при доступе клиента к серверам приложений с использованием криптографических процедур; при этом секретный ключ клиента должен обладать сертифицированной криптостойкостью и использоваться как для клиентской аутентификации, так и для формирования электронной цифровой подписи под электронным документом. При этом она должна была поддерживать средства

электронной цифровой подписи в соответствии с положениями Федерального закона «Об электронной цифровой подписи», обладать развитой системой администрирования, возможностью протоколирования событий и средствами анализа журналов событий. Отметим также, что система безопасности должна была обладать открытыми интерфейсами для подключения новых электронных приложений, не зависеть от платформ разработки и среды выполнения приложений front-office, при этом средства безопасности на стороне клиента должны были поддерживать концепцию тонкого клиента. При этом совокупная стоимость владения системой должна была быть минимальной.

Выработка корпоративного стандарта системы безопасности

Исходя из сформулированных требований к системе безопасности приложений front-office, в корпорации «НИКойл» была разработана четырехкомпонентная модель системы безопасности с использованием криптографических решений на базе инфраструктуры открытых ключей PKI. Это решение использует алгоритмы несимметричной криптографии, при этом объектами системы являются секретный и публичный ключи клиента и сертификат публичного ключа, сертифицированный третьей стороной — удостоверяющим центром (УЦ); иными словами, в системе используется схема с доверенной третьей стороной.

В процессе формирования концепции системы безопасности приложений front-office был проведен сравнительный анализ криптографических решений, предлагаемых на российском рынке, и выработан корпоративный стандарт на средства криптографии. В качестве стандарта было выбрано решение ООО «КриптоПро», использующее криптографический интерфейс компании Microsoft — Cryptographic Service Provider (CSP). Основанием для такого выбора послужило то, что, как было сказано выше, продукт «КриптоПро CSP» является решением, сертифицированным ФАПСИ, позволяет встраивать сертифицированные средства криптографии на базе «КриптоПро CSP» в любые клиентские и серверные приложения, функционирующие на платформе Windows, и, в отличие от базовых криптопровайдеров Windows, обеспечивает работу с ключами на гибких магнитных дисках, устройствах Touch Memory и E-token. Немаловажными факторами, которые учитывались при принятии данного решения, стали наличие документированного API и возможность гибкой настройки клиентских и серверных Windows-приложений для работы как с сертифицированными, так и с базовыми криптографическими средствами, интегрированными с платформой Windows.

Модель системы безопасности приложений front-office ИБГ «НИКойл»

В разработанной четырехкомпонентной модели системы безопасности основные функции, такие, как формирование шифрованного канала между клиентом и сервером, организация клиент-серверной аутентификации с использованием криптографических процедур, проверка принадлежности сертификата клиенту и наличия и количества подписей под документом, контроль целостности документа, проверка цепочки издателей отозванности и системной роли сертификата, проверка времени жизни секретного ключа, корректности последовательности подписей системных ролей под документом, квотирование доставки и архивирование документов, ведение журналов событий, связанных с открытием и закрытием сессий клиентов, получением/отправкой документов, результатами проверки электронных цифровых подписей, выполняются шлюзом безопасности прикладного уровня. В качестве платформы шлюза безопасности выбран Internet Security & Acceleration Server Enterprise Edition (сервер ISA) компании Microsoft, который является отказоустойчивым решением благодаря поддержке кластеров.

Схема взаимодействия компонентов системы безопасности для приложений front-office приведена на рисунке 1.

От шлюза безопасности электронный документ с электронной цифровой подписью также по защищенному каналу передается на сервер приложений, шифрование трафика от шлюза к серверу обеспечивает защиту документа от внутренних нарушителей, поэтому на сервере достаточно ограничиться проверкой целостности документа перед обработкой бизнес-системой. Проверку целостности и, возможно, добавление в него электронной цифровой подписи сервера приложений для отправки клиенту реализует второй компонент системы безопасности, встроенный непосредственно в бизнес-приложение.

Третий компонент системы безопасности обеспечивает на стороне клиента средства постановки/проверки подписи под электронным документом и средства аутентификации и формирования защищенного канала с использованием криптографических процедур. Процедуры работы с электронной подписью реализованы на языке VBscript, при этом средства аутентификации и формирования защищенного канала обеспечиваются протоколом TLS.

Для обеспечения клиентов и серверов приложений ключами шифрования используется четвертый компонент системы безопасности — удостоверяющий центр, который является основным

звеном системы управления инфраструктурой PKI. Программные компоненты корпоративного удостоверяющего центра используют сертифицированные криптографические средства на базе «КриптоПро CSP», а структура удостоверяющего центра позволяет задействовать его для выпуска сертификатов открытых ключей для применения в открытых информационных системах общего пользования. Составные части удостоверяющего центра разработаны на базе службы Certificate Authority операционной системы Windows 2000 Server и имеют собственные выделенные сервисы выпуска сертификатов.

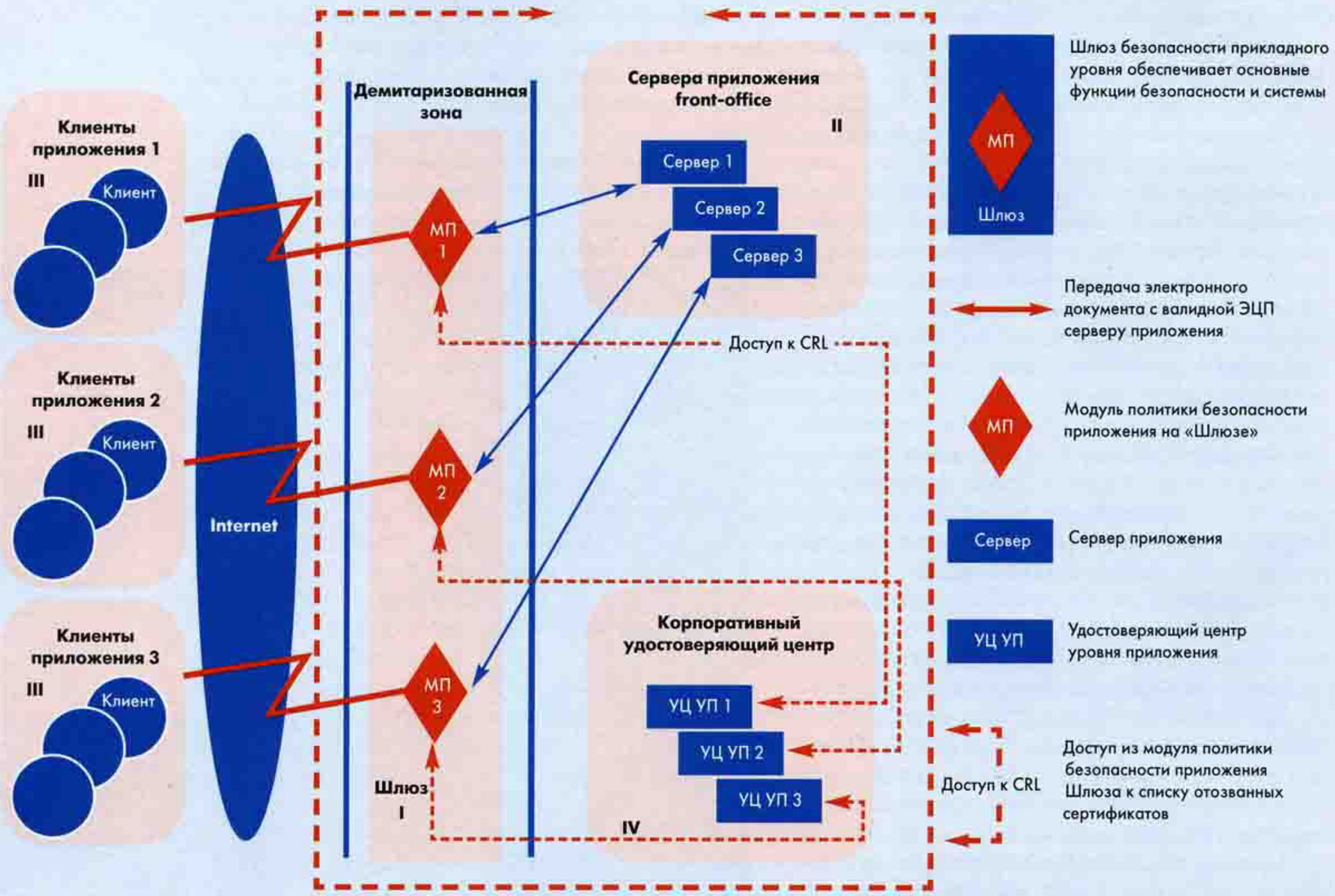
Описанный подход к построению системы безопасности приложений front-office был реализован при создании корпоративного удостоверяющего центра, построении системы безопасности и интеграции в нее существующих электронных приложений. Созданная система безопасности полностью удовлетворяет как предъявляемым к ней бизнес-требованиям, так и требованиям к ее функциональности; ПО реализует сертифицированные российские алгоритмы шифрования и подписи.

В качестве самостоятельного проекта в корпорации была создана электронная система обеспечения продаж паевых инвестиционных фондов, предоставляющая агентам паевых фондов Web-интерфейс для удаленного формирования заявок клиентов фонда на покупку/продажу паев инвестиционных фондов. В рамках этого проекта была реализована четырехкомпонентная модель системы безопасности, удостоверяющий центр которой был разработан в ООО «КриптоПро». В настоящее время электронная система обеспечения продаж паевых инвестиционных фондов эксплуатируется в промышленном режиме. До конца 2002 г. в корпорации будет введен корпоративный удостоверяющий центр, разработчиком которого также является ООО «КриптоПро».

О компании «НИКойл»

Финансовая корпорация «НИКойл» (www.nikoil.ru) — динамично развивающаяся финансовая структура,

Рисунок 1. Компоненты системы безопасности приложений front-office.



ведущая инвестиционный, коммерческий, частный банковский и страховой бизнес. Она является одним из крупнейших операторов российского фондового рынка — под ее управлением находится более 60% российских паевых фондов, объединяющих около 80 тыс. вкладчиков. Депозитарий ФК «НИКойл» занимает 8-е место по объему хранимых активов среди депозитариев России. Корпорация «НИКойл» также входит в десятку крупнейших консалтинговых групп России, в тройку лидеров по таким отраслям, как машиностроение и металлообработка, транспорт, энергетика, а также по наиболее конкурентным отраслям (машиностроение и металлообработка, транспорт, энергетика) и продуктам (стратегическое планирование и организационное развитие, маркетинг и отношения с общественностью).

Ядром корпорации является Акционерный банк «ИБГ НИКойл», входящий в число крупнейших кредитных учреждений России. Сегодня по размеру активов банк находится на 23-м месте в списке крупнейших банков страны и стабильно позиционируется в десятке самых прибыльных российских банков, занимая, по данным журналов «Эксперт» (№34(340) от 16.09.2002) и «Профиль» (№36 от 30.09.2002), лидирующие места по надежности.

О компании «Крипто-Про»

Компания «Крипто-Про» (www.cryptopro.ru) — динамично развивающийся разработчик средств защиты информации. Основными направлениями деятельности компании являются: разработка и внедрение криптографических средств, реализующих российские криптографические алгоритмы, в соответствии со стандартом Microsoft Cryptographic Service Provider, интеграция стандартизированных национальных криптографических алгоритмов с продуктами Microsoft, а также разработка и использование криптографических средств, поддерживающих Microsoft Public Key Infrastructure (PKI). Среди клиентов компании — аппарат Правительства Российской Федерации, Государственный таможенный комитет РФ, Банк Внешней торговли, ОАО «Альфа-Банк», ОАО «Лукойл», Администрация Президента Чувашской Республики, ЗАО «Управляющая компания НИКойл», ЗАО «Группа МДМ», ООО платежная Internet-система «Рапида», ОАО «Мосжилрегистрация» и др.

Компания «Крипто-Про» обладает, в частности, лицензиями ФАПСИ и Государственной технической комиссии при президенте РФ на право осуществления производства и проектирования средств защиты информации, на право осуществления деятельности по техническому обслуживанию и распространению шифровальных средств.

Среди продуктов компании «Крипто-Про» в первую очередь следует отметить криптопровайдер «КриптоПро CSP», разработанный ООО «Крипто-Про» и Государственным унитарным предприятием научно-техническим центром «Атлас» по техническому заданию, согласованному с ФАПСИ, а также удостоверяющий центр «КриптоПро УЦ» — комплекс программных средств, разработанных на основе служб сертификации операционной системы Windows 2000 Server и позволяющих в полном объеме реализовать инфраструктуру открытых ключей (PKI). Данная инфраструктура представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографическую защиту информации с сертификатами открытых ключей, а также для управления ими.

Криптопровайдер «КриптоПро CSP»

Средство криптографической защиты информации «КриптоПро CSP», разработанное совместно компанией «Крипто-Про» и ГУП НТЦ «Атлас», реализовано в соответствии со следующими российскими криптографическими алгоритмами:

- электронной цифровой подписи («ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма»);
- хеширования («ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хеширования»);
- шифрования и имитозащиты данных («ГОСТ 28147-89. Системы обработки информации. Защита криптографическая»).

Основная особенность «КриптоПро CSP» состоит в том, что это средство защиты, реализующее российские криптографические алгоритмы, разработано в соответствии с криптографическим интерфейсом CSP компании Microsoft. Благодаря этому, к стандартным приложениям, которые теперь могут использовать российские алгоритмы электронной цифровой подписи и шифрования, относятся центр Сертификации сертификатов открытых ключей X.509 (Microsoft Certification Authority), клиенты электронной почты Microsoft Outlook и Microsoft Outlook Express, средства формирования и проверки электронной цифровой подписи программных компонентов, распространяемых по сети (Microsoft Authenticode), и средства защиты Internet с использованием протокола TLS/SSL.

Средство криптографической защиты «КриптоПро CSP» имеет сертификат ФАПСИ СФ/114-0411 от 11 марта 2001 года.