

Механизмы безопасности в системе iBank 2 UA

(Версия 1.0)

Оглавление

| | |
|--|-----------|
| 1 Основные положения | 2 |
| Введение | 2 |
| Сущности и определения | 3 |
| Концепция и архитектура системы iBank 2 UA | 6 |
| Реализация и параметры используемых криптографических алгоритмов | 7 |
| IP-безопасность | 7 |
| 2 Подключение клиента к банку | 9 |
| Банковский вспомогательный Web-сервер | 10 |
| SoftUpdate и ЭЦП разработчика под Java-апплетами | 10 |
| 3 Защищенное взаимодействие между Java-апплетом и Сервером Приложения | 12 |
| Прикладной Протокол | 13 |
| Защищенный Сетевой Протокол | 14 |
| Долговременные и сессионные ключи | 15 |
| 4 Принципы безопасности при работе с документами | 18 |
| Передача клиентом документа в банк | 18 |
| Выгрузка документа из системы iBank 2 UA в учетную систему банка | 19 |
| Изменение статуса документа сотрудником банка | 20 |
| Получение клиентом отчета из банка | 20 |
| Проверка валидности Сертификата открытого ключа ЭЦП | 20 |
| Журналы событий | 21 |
| 5 Рекомендации банкам и клиентам | 23 |
| Рекомендации банкам | 23 |
| Рекомендации клиентам | 25 |
| 6 Источники дополнительной информации | 27 |

Глава 1

Основные положения

Введение

Система электронного банкинга iBank 2 UA предназначена для предоставления банком корпоративным и частным клиентам услуг электронного банкинга с поддержкой всех каналов доступа – Internet (онлайн и офлайн), WAP, SMS, телефон (голос, факс, модем). Система iBank 2 UA (программный комплекс) устанавливается в банке и позволяет обслуживать корпоративных и частных клиентов. Система активно используется крупнейшими многофилиальными системообразующими банками Украины.

iBank 2 UA относится к классу систем защищенного электронного документооборота. Обмен электронными документами происходит между банком и клиентом. Электронный документ, отправленный клиентом и полученный банком, является основанием для совершения финансовых операций.

Конечной целью всех атак на систему является:

- подмена (навязывание) злоумышленником электронного документа от имени одной из сторон;
- нарушение конфиденциальности документа (ознакомление с документом).

Для обеспечения аутентичности (доказательство авторства) и целостности документа в iBank 2 UA используется механизм электронной цифровой подписи (ЭЦП) под электронными документами. Именно электронный документ с ЭЦП является доказательной базой при разрешении конфликтной ситуации. В системе реализованы алгоритмы в соответствии с ГОСТ 34.310-95 (ЭЦП) и ГОСТ 34.311-95 (хеш-функция).

Для обеспечения конфиденциальности в iBank 2 UA используется механизм шифрования данных. Все электронные документы передаются через Интернет в зашифрованном виде. Шифрование данных осуществляется на сессионных ключах в соответствии с ГОСТ 28147-89 в режиме гаммирования.

Сущности и определения

В системе iBank 2 UA используются следующие сущности и определения:

- **Сервер Приложения iBank 2 UA** — серверное программное обеспечение системы электронного банкинга iBank 2 UA, устанавливаемое и эксплуатируемое в банке. Сервер Приложения (СП) обеспечивает обслуживание клиентов и сотрудников банка.
- **Шлюз** — программное обеспечение (ПО) для интеграции системы электронного банкинга iBank 2 UA с внешними учетными системами банка (с Оперднём, карточным процессингом и пр.).
- **Документ**. Под документом в системе электронного банкинга iBank 2 UA будем понимать любой финансовый документ, представленный в электронной форме. Финансовым документом является распоряжение клиента по управлению средствами в банке. Такое распоряжение всегда может быть представлено по установленной банком форме. Электронный документ всегда должен быть подписан одной или несколькими электронными цифровыми подписями (ЭЦП). Электронный документ с ЭЦП клиента имеет юридическую значимость наравне с традиционными бумажным финансовым документом.
- **Отчет**. Любой стандартный для системы iBank 2 UA отчет, сформированный сервером по запросу клиента. Например, выписка по банковскому счету за указанный период. Отчет всегда формируется сервером динамически по клиентскому запросу.
- **Прикладной запрос**. Прикладной запрос формируется клиентской компонентой одного из модулей или дополнительных сервисов системы iBank 2 UA и передается на банковский Сервер Приложения iBank 2 UA для исполнения. Запрос может содержать распоряжение на сохранение документа, получение отчета, получение служебной информации и т.д. Каждый запрос содержит идентификатор клиентского ключа. Перед обработкой любого запроса сервер проверяет права клиента на такой запрос.
- **Прикладной ответ**. Прикладной ответ формируется банковским Сервером Приложения, направляется клиентской компоненте и содержит результат обработки клиентского запроса. Это может быть признак успешности обработки запроса, финансовый отчет для клиента, блок служебной информации (например, справочник валют) и т.д.
- **Служебная информация** — дополнительная информация, передаваемая в клиентском запросе или возвращаемая сервером в ответе. Например: время сервера, список счетов клиента, запрос на сохранение реквизитов корреспондента и т.д.
- **Информационный поток** — совокупность всех пересылок прикладных запросов и прикладных ответов между клиентской компонентой и Сервером Приложения iBank 2 UA. Весь информационный поток всегда шифруется.
- **Шифрование** — криптографическое преобразование информации. В рамках защищенного документооборота – шифрование всего информационного потока с целью исключения доступа третьей стороны к передаваемой информации.
- **ЭЦП**. Электронная цифровая подпись является результатом криптографической обработки документа с использованием секретного ключа ЭЦП. ЭЦП служит для обеспечения аутентичности (подтверждения авторства и целостности) электронного документа.

- **Секретный ключ ЭЦП** — секретная последовательность длиной 32 байта, владельцем которой является только владелец ключа ЭЦП. Секретный ключ ЭЦП хранится владельцем в тайне и используется для формирования ЭЦП под электронным документом клиента. Дополнительно секретный ключ ЭЦП используется для аутентификации пользователя (клиента и сотрудника банка).
- **Открытый ключ ЭЦП** — последовательность длиной 128 байт, зависящая от секретного ключа ЭЦП. Открытый ключ ЭЦП предназначен для проверки корректности ЭЦП под электронным документом.
- **Сертификат открытого ключа ЭЦП** — блок информации, включающий в себя открытый ключ ЭЦП, параметры, срок и область действия открытого ключа ЭЦП, а также информацию о владельце открытого ключа ЭЦП, подписанный ЭЦП ответственного сотрудника банка. В сертификате содержится также информация об ответственном сотруднике банка, подписавшем данный сертификат.
- **Бумажный Сертификат открытого ключа ЭЦП** — документ, представленный на бумаге в печатном виде, содержащий открытый ключ ЭЦП в шестнадцатеричном виде, параметры, срок и область действия открытого ключа ЭЦП, а также информацию о владельце открытого ключа ЭЦП. Бумажный Сертификат открытого ключа ЭЦП заверяется подписью владельца и печатью организации (в случае корпоративного клиента) в присутствии ответственного банковского сотрудника. В бумажном Сертификате также присутствует информация об ответственном банковском сотруднике, зарегистрировавшем Сертификат открытого ключа ЭЦП в системе электронного банкинга iBank 2 UA.
- **Клиент.** Система iBank 2 UA поддерживает два типа клиентов:
 1. Корпоративные клиенты – юридические лица (организации) и частные предприниматели;
 2. Частные клиенты – физические лица, не занимающиеся предпринимательской деятельностью.
- **Клиентская компонента** — программное обеспечение системы электронного банкинга iBank 2 UA, используемое на стороне клиента для работы с финансовыми документами, отчетами и т.д. Клиентская компонента обеспечивает шифрование информационного потока при обмене с банковским Сервером Приложения, работу с ЭЦП и секретными ключами ЭЦП клиента. Клиентские компоненты по модулям:
 - АРМ **Регистратор** – загружаемый в Web-браузер клиента Java-апплет;
 - АРМ **Internet-Банкинг** – загружаемый в Web-браузер клиента Java-апплет;
 - АРМ **PC-Банкинг** – устанавливаемое клиенту Java-приложение;
 - АРМ **Mobile-Банкинг** – устанавливаемое клиенту .Net-приложение;
 - АРМ **Тикер** – устанавливаемое клиенту Java-приложение;
 - АРМ **SMS-Банкинг** – ветка Java-апплета Internet-Банкинга;
 - АРМ **WAP-Банкинг** – специальные wap-страницы;
 - АРМ **Phone-Банкинг** – услуга электронного банкинга посредством телефонной связи;
 - АРМ **Web-Банкинг** – специальные web-страницы;
 - АРМ **Корпоративный автоклиент** – устанавливаемое клиенту приложение.

- **Банковский АРМ.** Система электронного банкинга iBank 2 UA содержит четыре специализированных АРМа для банковских сотрудников:
 - АРМ **Администратор системы;**
 - АРМ **Администратор банка;**
 - АРМ **Операционист;**
 - АРМ **Регистратор банковских сотрудников.**

Концепция и архитектура системы iBank 2 UA

Система iBank 2 UA была разработана с учетом строгого соответствия концепции «тонкого клиента» — пользователю не требуется устанавливать никакого специализированного ПО. Для работы с системой клиенту необходим любой Web-браузер со встроенной виртуальной Java-машиной (JVM), соответствующей спецификации JDK 1.1 и выше. В качестве Web-браузера клиент может использовать:

- Microsoft Internet Explorer версии 4.0 и выше со встроенной Microsoft JVM версии 3272 и выше;
- Microsoft Internet Explorer версии 4.0 и выше с Sun Java Plugin;
- Netscape версии 6.0 и выше;
- Mozilla версии 1.0 и выше;
- Opera версии 5.0 и выше с Sun Java Plugin.

Для организации безопасной работы используются штатные средства защиты самого Web-браузера и встроенные в iBank 2 UA механизмы защиты информации.

Система iBank 2 UA реализована в классической трехзвенной архитектуре. Функции представительской компоненты выполняет загружаемый в Web-браузер клиента Java-апплет. В процессе работы апплет через защищенное соединение взаимодействует с банковским Сервером Приложения iBank 2 UA, в рамках которого исполняется вся бизнес-логика. Сервер Приложения, в свою очередь, общается с Сервером БД iBank 2 UA (Oracle, MS SQL или PostgreSQL), где хранится вся информация: документы клиентов, выписки, справочники, клиентские настройки, сертификаты открытых ключей ЭЦП, ресурсы, права и т.д.

В **Internet-Банкинге** работа клиента происходит в два этапа. На первом этапе клиент подключается к защищенному сайту банка и загружает в Web-браузер Java-апплет. Второй этап — работа клиента в Java-апплете и взаимодействие клиентского Java-апплета с банковским Сервером Приложения через защищенное соединение.

Работа в **PC-Банкинге** и **Mobile-Банкинге** начинается сразу со второго этапа — с взаимодействия клиентского Java-приложения с банковским Сервером Приложения iBank 2 UA.

Для обеспечения конфиденциальности в **Internet-Банкинге**, **PC-Банкинге** и **Mobile-Банкинге**, а также в дополнительных сервисах системы iBank 2 UA используется механизм шифрования данных. При взаимодействии через Интернет осуществляется шифрование и контроль целостности передаваемой информации, проводится криптографическая аутентификация сторон. Шифрование данных осуществляется на сессионных ключах в соответствии с ГОСТ 28147-89 в режиме гаммирования.

Для обеспечения конфиденциальности в **Web-Банкинге** используется криптографический протокол SSL, встроенный во все современные Web-браузеры. При взаимодействии через Интернет осуществляется шифрование и контроль целостности передаваемой информации, проводится криптографическая аутентификация клиентом банка.

В **WAP-Банкинге** для шифрования данных и аутентификации банка используются стандартные криптографические протоколы WTLS и SSL, для аутентификации клиента — идентификатор (логин) и пароль.

В **SMS-Банкинге** защита информации осуществляется стандартными для мобильной связи средствами. Для аутентификации клиента используются номер мобильного телефона, идентификатор и пароль.

В **Phone-Банкинге** шифрование голосовых и факсимильных сообщений по очевидным причинам невозможно. Для аутентификации клиента используются идентификатор и пароль, вводимые в тональном наборе.

Для проведения частными клиентами операций по списанию средств со счетов и карт в **Web-Банкинге**, **WAP-Банкинге** и **Phone-Банкинге** в качестве аналога собственноручной подписи клиента могут использоваться индивидуальные таблицы одноразовых паролей или аппаратные средства усиленной аутентификации — OTP-токены (One-Time Password) компаний Aladdin Knowledge Systems и VASCO Data Security International.

Реализация и параметры используемых криптографических алгоритмов

В систему iBank 2 UA встроена Java-криптобиблиотека «Стандарт-Ява», разработки ЗАО НПЦ «БИТиС». Java-криптобиблиотека «Стандарт-Ява» сертифицирована ДСТСЗИ СБУ. Сертификат соответствия № UA1.112.0135242-06 от 11 сентября 2006 г.

Криптобиблиотека реализована на языке Java, представлена в виде набора компактных Java-классов, встраиваемых в клиентские Java-апплеты, в клиентские и серверные Java-приложения. Криптобиблиотека предназначена для обеспечения защиты конфиденциальной информации, которая не является собственностью государства, от угроз нарушения конфиденциальности и целостности при помощи использования криптографических процедур, встроенных в прикладные программы. Криптобиблиотека реализует все режимы работы криптографических алгоритмов ГОСТ 28147-89 (шифрование), ГОСТ 34.310-95 (ЭЦП), ГОСТ 34.311-95 (хеш-функция).

Криптобиблиотека «Стандарт-Ява» встроена и распространяется в составе системы iBank 2 UA на основании Договора № 1 от 30 января 2003 г. «На передачу Программы для ЭВМ «Программное изделие «Стандарт-Ява». Классы криптографических преобразований между ООО «БИФИТ» и ЗАО НПЦ «БИТиС».

Система iBank 2 UA всегда поставляется со встроенной сертифицированной криптобиблиотекой «Стандарт-Ява». Специально приобретать для каждого клиента или для каждого рабочего места Лицензию на средство КЗИ не нужно. Для проведения работ по разработке средств КЗИ, защищенных систем, работ по техническому обслуживанию и распространению шифрованных средств компания «БИФИТ» имеет Лицензию ДСТСЗИ СБУ.

IP-безопасность

При внедрении системы iBank 2 UA всегда проводятся изменения текущей политики IP-безопасности банка. Серверы системы iBank 2 UA размещаются в отдельном сетевом сегменте с контролируемым на межсетевом экране доступом из Интернета и внутренней защищенной сети банка. Также при внедрении системы iBank 2 UA всегда проводится тщательная настройка операционных систем на серверах системы iBank 2 UA – исключается поддержка неиспользуемых протоколов, сетевых сервисов и служб. На серверах системы iBank 2 UA запрещается сетевой доступ к файловой системе, задействуются встроенные в ОС механизмы аудита.

Правильно спроектированная и четко реализованная политика IP-безопасности, постоянный IP-мониторинг позволяют обеспечить гарантированный уровень защиты системы iBank 2 UA и внутренней сети банка.

Глава 2

Подключение клиента к банку

Работа клиента начинается с подключения к Web-серверу банка. Клиент в Web-браузере указывает полный URL банковского Web-сервера, включая тип используемого протокола HTTPS (прикладной протокол HTTP поверх криптографического протокола SSL).

Например, <https://ibank.bankname.com>.

Загружаемые в браузер html-страницы, конфигурационные XML-файлы, Java-апплеты и другие данные являются открытыми. На этом этапе не требуется ввода идентификаторов и паролей для аутентификации. Поскольку клиент не загружает секретные параметры, то шифровать трафик на этапе подключения необязательно. Атаки злоумышленника на этапе подключения могут быть направлены:

- на подмену банковского Web-сервера;
- на модификацию загружаемых в Web-браузер клиента стартовых html-страниц;
- на модификацию загружаемых в Web-браузер клиента конфигурационных XML-файлов;
- на модификацию загружаемых в Web-браузер клиента Java-апплетов.

Конечная цель атак — подмена загружаемого к клиенту Java-апплета с последующим хищением секретного ключа ЭЦП клиента.

Для предотвращения указанных атак на этапе подключения используется встроенный в Web-браузеры протокол SSL, обеспечивающий:

- гарантированное подключение клиента к банковскому Web-серверу;
- целостность загружаемой к клиенту с банковского Web-сервера информации (html-страницы, конфигурационные XML-файлы, Java-апплеты и пр.).

При работе через протокол SSL Web-браузер клиента обеспечивает аутентификацию банковского Web-сервера, сравнивая доменное имя в введенном клиентом URL с доменным именем, указанным в сертификате. Также SSL обеспечивает целостность всех загружаемых в Web-браузер данных. Наличие или отсутствие экспортных ограничений в реализации криптографического протокола SSL в ранних версиях Web-браузеров никак не сказывается на уровне безопасности, т. к. указанные ограничения распространялись исключительно на алгоритмы шифрования данных и длины сеансовых ключей, и никак не влияли на механизмы аутентификации Web-сервера и обеспечения целостности передаваемых данных.

Банковский вспомогательный Web-сервер

К надежности и защищенности банковского Web-сервера, к его администрированию предъявляются исключительно высокие требования. В связи с этим в Сервер Приложения iBank 2 UA встроен вспомогательный Web-сервер, основанный на ядре сервлетного движка Tomcat с необходимыми модификациями и функциональными ограничениями. Основным предназначением данного вспомогательного Web-сервера является исключение даже возможности потенциальных атак на модификацию html-страниц, Java-апплетов и других ресурсов. В Web-сервере используются реализации криптографического протокола SSL компании Sun Microsystems.

В составе системы iBank 2 UA поставляется утилита, предназначенная для генерации секретного и открытого ключей (SSL) вспомогательного Web-сервера, формирования запроса на получение Сертификата X.509, импортирования сертификата, выданного Сертификационным Центром.

Сертификат X.509 для Web-сервера необходимо получать у одного из мировых Сертификационных Центров. Более подробную информацию о получении SSL-сертификата можно найти в документе **Инструкция по получению SSL-сертификата**.

SoftUpdate и ЭЦП разработчика под Java-апплетами

Во все распространенные Web-браузеры встроены механизмы ускорения загрузки Java-апплетов при повторном подключении пользователя. В Microsoft Internet Explorer этот механизм называется SoftUpdate, в Netscape — SmartUpdate. Механизмы ускорения загрузки (далее для краткости — SoftUpdate) различаются в деталях, но решают единую задачу. Для использования механизма SoftUpdate в html-страницы встраивается несколько строк кода на JavaScript.

При самом первом подключении Web-браузер загружает с Web-сервера Java-апплет (в виде CAB-архива для MS Internet Explorer или JAR-архива для остальных типов браузеров) и сохраняет на локальном диске пользователя в одном из служебных подкаталогов браузера.

При последующих повторных подключениях Web-браузер сравнивает ранее загруженную версию Java-апплета, сохраненную в служебном подкаталоге, с текущей версией на Web-сервере. Если версии совпадают, то используется ранее загруженная версия Java-апплета. Если на Web-сервере более новая версия Java-апплета, то Web-браузер автоматически загружает, сохраняет в служебном подкаталоге и в дальнейшем использует более новую версию.

SoftUpdate используется в iBank 2 UA по умолчанию. В составе системы также есть стартовые html-страницы для загрузки Java-апплетов без использования SoftUpdate.

В iBank 2 UA все загружаемые к клиенту Java-апплеты подписаны ЭЦП компании-разработчика. Механизм проверки ЭЦП разработчика под Java-апплетами также является стандартным и встроен во все распространенные Web-браузеры.

Проверка ЭЦП разработчика (компании «БИФИТ») осуществляется на основании Сертификата X.509 разработчика, выданного мировым Сертификационным Центром Thawte Consulting — www.thawte.com. Корневые Сертификаты мировых Сертификационных Центров присутствуют в составе дистрибутивов всех типов и версий Web-браузеров.

ЭЦП разработчика под Java-апплетами используется:

- Для обеспечения целостности и аутентичности Java-апплетов, загруженных и хранимых в служебном подкаталоге Web-браузера при использовании механизма SoftUpdate (защита от атак по модификации файлов с Java-апплетами, хранимых на компьютере клиента);
- Для предоставления виртуальной Java-машиной Web-браузера расширенных привилегий для Java-апплета: работа с локальными дисками клиента (для доступа к дискете/диску с Хранилищем секретных ключей ЭЦП клиента), печать на принтере, взаимодействие с хостами, IP-адреса которых отличны от IP-адреса вспомогательного Web-сервера.

Глава 3

Защищенное взаимодействие между Java-апплетом и Сервером Приложения

Инициатором защищенного взаимодействия между клиентским Java-апплетом и банковским Сервером Приложения всегда является Java-апплет. Как только появляется необходимость передать в банк документ или получить информацию из банка, клиентский Java-апплет осуществляет защищенное взаимодействие с банковским Сервером Приложения.

Защищенное взаимодействие разбито на два уровня: верхний уровень — Прикладной Протокол, и нижний уровень — Защищенный Сетевой Протокол.

| Уровень | Функция |
|-----------------------------|---|
| Прикладной протокол | Аутентификация Клиента Механизм ЭЦП Прикладные запросы и ответы |
| Защищенный Сетевой Протокол | Шифрование данных Обеспечение целостности данных Аутентификация Банка |

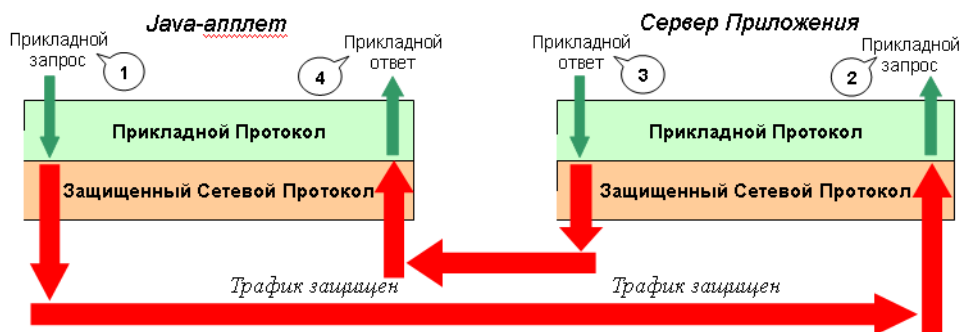


Рис. 3.1. Защищенное взаимодействие между Java-апплетом и Сервером Приложения

Далее подробно рассматриваются **Прикладной Протокол** и **Защищенный Сетевой Протокол**.

Прикладной Протокол

Механизмы аутентификации пользователя и ЭЦП реализованы в Прикладном Протоколе. Прикладной Протокол строится по следующему принципу:

УСТАНОВКА СОЕДИНЕНИЯ \implies ЗАПРОС \implies ОТВЕТ \implies ЗАКРЫТИЕ СОЕДИНЕНИЯ

Транзакция выглядит следующим образом:

1. Java-апплет открывает соединение с Сервером Приложения;
2. Java-апплет формирует Прикладной запрос и отправляет его Серверу Приложения;
3. Сервер Приложения принимает Прикладной запрос и обрабатывает его;
4. Сервер Приложения формирует Прикладной ответ и отправляет Java-апплету;
5. Java-апплет принимает Прикладной ответ и обрабатывает его;
6. Java-апплет закрывает соединение с Сервером Приложения.

Прикладной запрос состоит из заголовка и области данных. В заголовке прикладного запроса передаются следующие параметры:

- Код прикладного запроса;
- Идентификатор открытого ключа ЭЦП клиента;
- Сеансовый пароль длиной 32 байта;
- Временная метка;
- Длина области данных.

В области данных передаются значения параметров прикладного запроса. ЭЦП клиента также является параметром в области данных прикладного запроса (как номер документа, дата документа и пр.).

Прикладной ответ также состоит из заголовка и области данных. В заголовке возвращаются код ошибки прикладного ответа и длина области данных. В области данных возвращаются значения параметров прикладного ответа.

Сеансовый пароль генерируется Java-апплетом на этапе инициализации (генерация осуществляется с помощью криптографического генератора псевдослучайных чисел SecureRandom) и устанавливается при первом обращении Java-апплета к банковскому Серверу Приложения с использованием механизма ЭЦП клиента под сеансовым паролем. Длина пароля – 32 байта – обеспечивает 2^{256} комбинаций. Вероятность подбора сеансового пароля $\sim 10^{-78}$.

Время жизни сеансового пароля задается в настройках Сервера Приложения (по умолчанию 30 минут). По истечении времени жизни Сервер Приложения потребует от клиента провести установку сеансового пароля заново с использованием ЭЦП клиента.

Двухфазная аутентификация (с помощью ЭЦП клиента при установлении соединения и с помощью сеансового пароля в процессе взаимодействия) позволяет сохранить гарантированную защищенность, как если бы для аутентификации клиента каждый прикладной запрос подписывался ЭЦП (длина сеансового пароля, как и длина секретного ключа ЭЦП клиента, равна

32 байтам), и при этом существенно снизить нагрузку на Сервер Приложения, исключив процедуру проверки ЭЦП под каждым прикладным запросом.

Прикладные запросы с ЭЦП клиента не используются при разрешении конфликтных ситуаций (единственно необходимым и достаточным доказательным материалом при разрешении конфликтных ситуаций являются электронные документы с ЭЦП клиента). Информация о прикладных запросах сохраняется в журналах системы (см. [Журналы событий](#)).

В Прикладном Протоколе используются следующие криптографические алгоритмы:

- ГОСТ 34.310-95 — процедура формирования и проверки Электронной Цифровой Подписи. Имеет три фиксированных предварительно вычисленных и жестко прописанных открытых параметра: a , q , p . Для ключей ЭЦП пользователя длина параметров a и p равна 1024 битам;
- ГОСТ 34.311-95 — процедура вычисления хэш-функции. Таблицы замен фиксированы, взяты из контрольного примера ГОСТа. Используется в процедуре формирования и проверки ЭЦП.

Для работы Прикладного Протокола необходима пара ключей ЭЦП клиента. Секретный ключ ЭЦП клиента хранится в файле в зашифрованном на пароле виде. Открытый ключ ЭЦП клиента хранится в банке в Сервере БД системы iBank 2 UA в виде Сертификата, заверенного банковским администратором. Также в банке хранится заверенный подписями руководителей и печатью организации бумажный Сертификат открытого ключа ЭЦП клиента.

Защищенный Сетевой Протокол

Защищенный Сетевой Протокол выполняет следующие функции:

1. Обеспечивает шифрование данных, передаваемых между Java-апплетом и Сервером Приложения;
2. Обеспечивает целостность данных, передаваемых между Java-апплетом и Сервером Приложения;
3. Обеспечивает аутентификацию Сервера Приложения Java-апплетом.

Защищенный Сетевой Протокол является, фактически, модернизированным протоколом SSL v.3 с упрощенной процедурой согласования сеансовых ключей и с заранее определенными используемыми криптографическими алгоритмами, длинами ключей и другими параметрами.

Защищенный Сетевой Протокол позволяет клиенту, при необходимости, работать и через HTTP Proxy-сервер (MS Proxy, WinGate, Win Proxy, Squid и др.). Используется тот же механизм HTTP Proxy-сервера, как и при работе протокола SSL. Поддерживаются режимы работы через Proxy-сервер с аутентификацией и без аутентификации.

При необходимости Защищенный Сетевой Протокол может быть заменен на любой другой защищенный протокол, работающий поверх TCP, однако для этого требуется вносить программные модификации в систему iBank 2 UA. Например, может использоваться реализация SSL v.3 браузера.

Главные достоинства Защищенного Сетевого Протокола — чрезвычайно низкий объем служебных данных, передаваемых в процедуре согласования сеансовых ключей, а также невысокая

нагрузка на процессоры банковского сервера, возникающая в процессе защищенного взаимодействия Java-апплетов с Сервером Приложения.

В процедуре согласования сеансовых ключей используется алгоритм RSA с длиной ключа 1024 бита. При передаче данных вся информация шифруется на сеансовых ключах по ГОСТ 28147-89 в режиме гаммирования. Для обеспечения целостности данных используется ГОСТ 28147-89 в режиме имитовставки.

В Защищенном Сетевом Протоколе используются следующие криптографические алгоритмы:

- RSA-1024 — асимметричный криптографический алгоритм с модулем N длиной 1024 бита. Используется в процедуре согласования сеансовых ключей шифрования и контроля уникальности сессии. Java-апплет шифрует информацию на Открытом ключе шифрования банка. Сервер Приложения расшифровывает информацию на Секретном ключе шифрования банка. Для ускорения работы процедуры вычисления модульной экспоненты со стороны Java-апплетов используется «короткая» публичная экспонента, равная 65537. Для ускорения работы со стороны сервера используются секретные числа P и Q (модуль — $N = P \cdot Q$);
- ГОСТ 28147-89 — симметричный алгоритм шифрования. Используется Java-апплетами и Сервером Приложения для шифрования передаваемых данных в режиме гаммирования, а также для вычисления имитовставки. Длины сессионных ключей шифрования и выработки имитовставки — 32 байта.

Для работы Защищенного Сетевого Протокола необходима одна пара ключей шифрования банка, используемая в процедуре согласования сеансовых ключей (RSA-1024). Пара ключей шифрования банка хранится на Сервере Приложения. Секретный ключ шифрования банка используется Сервером Приложения в процессе взаимодействия с Java-апплетами. Открытый ключ шифрования банка загружается клиенту со вспомогательного Web-сервера (файл `public_gsl`) через браузерный HTTPS и используется Java-апплетом в качестве одного из параметров защищенного взаимодействия.

Долговременные и сессионные ключи

Все ключи, используемые в iBank 2 UA, можно разделить на две группы: сеансовые ключи и долговременные ключи. К сеансовым ключам относятся:

- Сессионные ключи шифрования данных. Алгоритм шифрования — ГОСТ 28147-89;
- Сессионные ключи формирования имитовставки. Алгоритм — ГОСТ 28147-89

К долговременным ключам относятся:

- Секретный и открытый ключи ЭЦП клиентов. Алгоритм ЭЦП — ГОСТ 34.310-95;
- Секретный и открытый ключи ЭЦП операционистов и администраторов филиалов. Алгоритм ЭЦП — ГОСТ 34.310-95;
- Секретный и открытый ключи шифрования банка. Алгоритм шифрования — RSA с модулем 1024 бита. Используется в фазе согласования сеансовых ключей.

Сессионные ключи шифрования данных и формирования имитовставки имеют длину 32 байта и генерируются Java-апплетом каждый раз заново для каждой новой транзакции.

Для генерации сессионных ключей используется криптографический генератор псевдослучайных чисел SecureRandom. В качестве стартового вектора используется массив байт, снимаемых с программного датчика случайных чисел SeedGenerator (см. исходные тексты реализации класса SeedGenerator в JDK 1.1.8).

Ключи ЭЦП клиентов. Клиент может иметь любое необходимое ему количество пар ключей ЭЦП. Одновременно может быть несколько активных (действующих) пар ключей ЭЦП. Предусмотрено группирование ключей ЭЦП: 1-ая подпись, 2-ая подпись и т.д. Банковским администратором настраивается до 8-ми групп ЭЦП по каждому клиенту.

Клиент в рамках Java-апплета **Регистратор** самостоятельно генерирует свою пару ключей ЭЦП. Для генерации пары ключей ЭЦП клиента используется криптографический генератор псевдослучайных чисел SecureRandom. В качестве стартового вектора используется массив байт, снимаемых с программного датчика случайных чисел SeedGenerator, и массив байт, формируемый биологическим датчиком случайных чисел, набирающим случайность из 1024 измерений координат указателя мыши и текущего времени в миллисекундах в моменты возникновения событий, вызванных движением указателя мыши.

После генерации пары ключей ЭЦП клиента, открытый ключ ЭЦП клиента из Java-апплета **Регистратор** по защищенному соединению передается Серверу Приложения в банк и предварительно регистрируется. По защищенному соединению Сервер Приложения возвращает Java-апплету **Регистратор** идентификатор предварительно зарегистрированного открытого ключа ЭЦП клиента.

После ввода в Java-апплете **Регистратор** пароля секретный ключ ЭЦП клиента зашифровывается (ГОСТ 28147-89) на хеш-функции (ГОСТ 34.311-95) от введенного клиентом пароля и идентификатора ключа и сохраняется на дискете в файле хранилища секретных ключей ЭЦП клиента. Каждому секретному ключу ЭЦП клиента, размещенному в Хранилище ключей, пользователь присваивает наименование для дальнейшего использования ключа в работе. При личном посещении банка клиент подписывает Договор на обслуживание в системе и заверяет бумажный Сертификат своего открытого ключа ЭЦП.

Все открытые ключи ЭЦП клиентов хранятся в банке, в Сервере БД системы iBank 2 UA в виде Сертификатов открытых ключей ЭЦП клиентов.

Секретный ключ ЭЦП клиента используется для аутентификации клиента и для формирования ЭЦП клиента под финансовыми документами и другими исходящими от клиента распоряжениями.

Открытый ключ ЭЦП клиента используется банком для аутентификации клиента и для проверки ЭЦП клиента под финансовым документом. Проверка ЭЦП клиента осуществляется Сервером Приложения в момент подписи клиентом документов, а также Шлюзом при выгрузке документов в АБС банка.

Ключи ЭЦП операционистов и администраторов филиала. Банковский операционист и администратор филиала могут иметь необходимое им количество пар ключей ЭЦП.

Генерация ключей операциониста и администратора филиала осуществляется с помощью Java-апплета **Регистратор банковских сотрудников**, аналогичного АРМ **Регистратор** для клиентов. Секретные ключи ЭЦП операционистов и администраторов филиалов хранятся в Хранилище в файле на съёмном носителе. Открытые ключи ЭЦП операционистов и администраторов филиалов хранятся в Сервере БД iBank 2 UA.

Пара ключей шифрования банка генерируется банковским администратором и может меняться банком с произвольной частотой (требует перезапуска Сервера Приложения).

В состав системы iBank 2 UA входит программа, которая генерирует пару ключей шифрования банка и сохраняет ключи в файле `%ibank_home%\conf\gs1keystore` (`%ibank_home%` – каталог, в который установлен Сервер Приложения iBank 2 UA). Секретный ключ шифрования банка используется Сервером Приложения в процессе взаимодействия с Java-апплетами.

Более подробно о генерации ключей можно прочитать в документе ***Установка системы iBank 2 UA под ОС Windows/Unix***.

Открытый ключ шифрования банка хранится в файле `%ibank_home%\webapps\ROOT\public_gs1` на банковском сервере. Данный ключ загружается Java-апплетом в процессе инициализации через браузерный HTTPS со вспомогательного Web-сервера банка и используется для взаимодействия с банковским Сервером Приложения.

С целью минимизации вычислительных затрат на стороне клиента в качестве публичной экспоненты используется пятое число Ферма $65537 = 2^{16} + 1$.

Глава 4

Принципы безопасности при работе с документами

Передача клиентом документа в банк

Клиент (корпоративный или частный) может создавать, редактировать и сохранять документы в одном из клиентских АРМов. При сохранении документа проверяются:

- Наличие у клиента прав на работу с данным типом документа;
- Соответствие реквизитов клиента в документе текущим реквизитам клиента;
- Принадлежность клиенту счетов, указанных в документе;
- Правильность заполнения полей документа.

Документ подписывается на стороне клиента криптобиблиотекой, встроенной в клиентский АРМ. Подпись документов возможна во всех клиентских АРМах, кроме **Web-Банкинга** и **WAP-Банкинга** (в этих двух модулях нет механизма ЭЦП финансовых документов). Для формирования ЭЦП подписываемый документ представляется в формате XML. Подписываются все поля документа (наименование и значение полей), присутствующие в XML-описании данного типа документа. При формировании ЭЦП клиента используется время банковского Сервера Приложения. Все клиентские АРМы, кроме **Mobile-Банкинга**, **Web-Банкинга** и **WAP-Банкинга** реализованы на Java. ЭЦП формируется клиентским АРМом, исполняемым в рамках виртуальной Java-машины на стороне клиента. Подменить подписываемые данные в памяти виртуальной Java-машины практически неосуществимо.

В случае **Mobile-Банкинга** клиентская компонента реализована на C# и для работы требует наличия на КПК или коммуникаторе клиента Microsoft .NET Compact Framework (виртуальной машины для исполнения байт-кода, скомпилированного из исходных текстов, написанных на C#). В составе PocketPC 2003 и Windows Mobile 5.0 виртуальная машина уже есть.

Если под документом требуется несколько ЭЦП для рассмотрения документа банком (в случае корпоративных клиентов), сотрудники корпоративного клиента – владельцы соответствующих ЭЦП – с помощью своих АРМов каждый подписывают документ. При каждом подписании документа проверяются:

- Принадлежность сертификата открытого ключа ЭЦП клиента подписывающему клиенту;
- Валидность сертификата открытого ключа ЭЦП клиента;

- Наличие в сертификате открытого ключа ЭЦП клиента прав на подпись данного типа документа;
- Отсутствие под документом других подписей той же группы;
- Наличие у клиента прав на работу с данным типом документа;
- Соответствие реквизитов клиента в документе текущим реквизитам клиента;
- Принадлежность клиенту счетов, указанных в документе.

Когда документ собирает необходимое число подписей, документ либо автоматически выгружается в соответствующую учетную систему банка (в Опердень, в карточный процессинг и т.д.), либо попадает на рассмотрение сотрудника банка, работающего с документами клиентов в iBank 2 UA (зависит от стратегии обработки приходящих от клиентов документов).

Выгрузка документа из системы iBank 2 UA в учетную систему банка

Первичный документ с ЭЦП клиента всегда хранится в Сервере БД системы iBank 2 UA. Выгрузку документа в учетную систему банка – в Опердень, карточный процессинг и пр. – осуществляет Шлюз. При создании и сохранении новому документу присваивается статус **Новый**. Пока документ не набрал необходимое количество подписей, документ имеет статус **Подписан** (клиент может проверить дату, время подписи и кто подписывал). После того, как все необходимые подписи поставлены – документ приобретает статус **Доставлен**. Далее начинает работать Шлюз на стороне банка. При выгрузке документа Шлюз проверяет:

- Принадлежность документа данному клиенту;
- Наличие у клиента прав на работу с данным типом документа;
- Соответствие реквизитов клиента в документе текущим реквизитам клиента;
- Принадлежность клиенту счетов, указанных в документе;
- Наличие у клиента прав на работу со счетами, указанными в документе;
- Принадлежность сертификата открытого ключа ЭЦП данному клиенту;
- Валидность сертификатов открытых ключей ЭЦП клиента;
- Корректность всех ЭЦП под документом;
- Соответствие количества и групп подписи ЭЦП под документом указанному в правах клиента на работу с данным типом документа.

Если все проверки прошли успешно, Шлюз в этой же транзакции форматирует и выгружает документ в учетную систему банка в согласованном формате. По согласованию с банком в Шлюз могут быть встроены дополнительные механизмы защиты информации (ЭЦП, шифрование) для защиты выгружаемых документов.

На практике во многих внедрениях системы iBank 2 UA в Шлюзы встраиваются внешние средства КЗИ – от сертифицированных ДСТСЗИ до публичных свободно-распространяемых криптопровайдеров – которые поддерживаются учетными системами банков. При согласовании с

банком выгрузки документов из системы iBank 2 UA в учетные системы банка необходимо учитывать, что формирование Шлюзом ЭЦП под документом процесс ресурсоемкий, сильно поглощающий вычислительные (процессорные) ресурсы. При этом в учетной системе банка ЭЦП под документов будет проверяться, что создает не меньшую вычислительную нагрузку на сервер учетной системы. При небольшом потоке выгружаемых документов в 2-3 документа в секунду нагрузка будет незначительна. При большом потоке в 50-70 документов в секунду – критична для Шлюза и учетной системы.

При согласовании выгрузки документов механизм ЭЦП Шлюза под документом следует использовать аккуратно – т. е. только в тех случаях, когда существует фаза пребывания документа в незащищенном виде. Например, в виде файла. И при этом требуется наличие возможности разбора конфликтной ситуации между участниками (между Шлюзом и учетной системой банка). При этом и Шлюз, и учетная система банка должны хранить контрольные архивы – запросы/ответы противоположной стороны с ЭЦП противоположной стороны.

Изменение статуса документа сотрудником банка

Сотрудник банка в АРМе **Операционист** может осуществлять просмотр и печать документов, добавление комментариев к ним. Операционист может просмотреть каждый документ (с целью проверки правильности заполнения документа) и проверить корректность ЭЦП под ним. По результатам проверок сотрудник банка имеет возможность изменить статус документа. Более подробно об изменении статусов объектов читайте в документе **Система iBank 2 UA. Руководство операциониста корпоративных клиентов**.

Получение клиентом отчета из банка

От банка к клиенту направляются отчеты и письма. К отчетам можно отнести:

- выписки по счетам за произвольный период;
- оборотно-сальдовые ведомости за произвольный период;
- отчеты по бюджетированию;
- курсы валют.

Отчеты формируются динамически на основании информации о проводках в Сервере БД системы iBank 2 UA. В стандартной версии динамически формируемые Сервером Приложения iBank 2 UA по запросам клиента отчеты не подписываются ЭЦП банка, но передаются с использованием механизмов КЗИ. В индивидуальных версиях по согласованию с банками выбранные типы отчетов могут направляться из банка к клиенту вместе с ЭЦП банка с возможностью последующей выгрузки в файл подписанных банком документов.

Проверка валидности Сертификата открытого ключа ЭЦП

Проверка валидности сертификата открытого ключа ЭЦП осуществляется каждый раз перед использованием данного сертификата для проверки ЭЦП под документом/прикладным запросом. Проверка валидности сертификата открытого ключа ЭЦП осуществляется двумя службами:

- Сервером Приложения iBank 2 UA при подписи клиентом исходящих документов и при аутентификации клиента;

- Шлюзом при выгрузке в учетную систему банка пришедших от клиентов документов.

Перед использованием сертификата открытого ключа ЭЦП проверяются:

- Принадлежность сертификата субъекту;
- Период действия сертификата;
- Текущий статус сертификата;
- Область применения сертификата;
- Корректность открытого ключа ЭЦП;
- Права издателя, подписавшего сертификат;
- ЭЦП издателя под сертификатом.

Журналы событий

Для разрешения конфликтных ситуаций в систему iBank 2 UA встроен механизм ЭЦП клиента под финансовым документом. Доказательными материалами при разрешении конфликтной ситуации являются электронные документы с ЭЦП клиентов, которые хранятся в банке, на Сервере БД iBank 2 UA.

Для полного восстановления действий клиентов и произошедших событий, в iBank 2 UA встроен механизм журнализации. Журналы событий не являются доказательными материалами при разрешении конфликтных ситуаций, но позволяют максимально подробно восстановить весь ход произошедших событий.

В каталоге %ibank_home%\logs СП сохраняет отдельные файлы для каждого пользовательского модуля. Ошибки и события системы фиксируются в отдельных файлах. Исходя из этого, имя файла журнала строится следующим образом:

<служебное название пользовательского модуля> + знак подчеркивания "_" + event (для журнала событий) или **error** (для журнала ошибок).

В системе ведутся следующие журналы событий:

| № | Наименование файла логов | Описание |
|---|-----------------------------|--|
| 1 | access.log | Обращения к встроенному веб-серверу iBank 2 UA |
| 2 | activemq.log | Модуль ActiveMQ (рассылка сообщений SMS – Банкинга) |
| 3 | admin_event(error).log | Модуль Администратор банка ¹ |
| 4 | autoclient_event(error).log | Модуль Корпоративный автоклиент |
| 5 | dbcreator.log | Утилита по созданию SQL-скриптов для выбранного типа СУБД, которые формируют БД iBank 2 UA |
| 6 | handy_event(error).log | Модуль Mobile — Банкинг для юридических лиц |
| 7 | ibank_event(error).log | Модуль Internet — Банкинг для юридических лиц |

¹АРМ **Администратор системы**, функционируя независимо от СП, выводит сообщения об ошибках исключительно на консоль.

| | | |
|----|------------------------------|--|
| 8 | ipfilter_event.log | Механизм IP – фильтрации |
| 9 | ip_filter_filling.log | Загрузка в БД таблицы IP-фильтра (утилита load_ipfilter_info) |
| 10 | isida_event(error).log | Модуль Операционист юридических лиц |
| 11 | jerry.log | Сервер Приложения |
| 12 | load_res.log | Загрузка программных ресурсов для пользовательских апплетов в БД iBank 2 UA (утилита load_res) |
| 13 | load_struct_corporate.log | Загрузка структурированных платежей юридических лиц (утилита load_structref) |
| 14 | load_struct_private.log | Загрузка структурированных платежей физических лиц (утилита load_structref) |
| 15 | make_dist.log | Формирование клиентских дистрибутивов РС – Банкинга, Корпоративного автоклиента (утилита make_dist) |
| 16 | make_dist_ticker.log | Формирование клиентского дистрибутива Тикера для юридических лиц (утилита make_dist) |
| 17 | mfo.log | Импорт справочника МФО в БД iBank 2 UA (утилита load_mfo) |
| 18 | msinker_event(error).log | Модуль РС – Банкинг. Центр Финансового Контроля |
| 19 | multiclient_event(error).log | Модуль Internet – Банкинг. Центр Финансового Контроля |
| 20 | pegasus_event(error).log | Модуль SMS – Банкинг |
| 21 | pibank_event(error).log | Модуль Internet – Банкинг для физических лиц |
| 22 | pisida_event(error).log | Модуль Операционист физических лиц |
| 23 | psinker_event(error).log | Модуль РС – Банкинг для физических лиц |
| 24 | rates.log | Импорт курсов валют, рассылаемых НБУ, и курса конвертации банка в БД iBank 2 UA (утилита load_rates) |
| 25 | registry_event(error).log | Модуль Регистратор |
| 26 | sinker_event(error).log | Модуль РС – Банкинг для юридических лиц |
| 27 | sirena_event(error).log | Модуль Phone – Банкинг |
| 28 | swift.log | Импорт справочника SWIFT в БД iBank 2 UA (утилита load_swift) |
| 29 | ticker_event(error).log | Модуль Тикер для юридических лиц |
| 30 | wap_event(error).log | Модули WAP – Банкинг для юридических лиц и WAP – Банкинг для физических лиц |

В таблице выше приведены файлы журналов серверной части, т. е. только самого Сервера Приложения. В этих журналах *не фиксируются ошибки*, которые возникают на стороне клиента. Файлы журналов клиентской части ведутся приложениями, установленными на стороне клиента. Для файлов журналов клиентское приложение, например, РС-Банкинг создает в каталоге установки подкаталог log.

Более подробно о структуре каталогов и назначении файлов можно узнать в документе **Файловая структура Сервера Приложения iBank 2 UA**.

Также в iBank 2 UA ведется история документов — журналируется информация о создании документа, об изменении статуса документа. В истории документов сохраняется информация о субъекте, породившем событие, о времени и дате события.

Глава 5

Рекомендации банкам и клиентам

Рекомендации банкам

Во избежание конфликтных ситуаций с клиентами банка, а также для исключения атак на конфиденциальную информацию о клиентах со стороны злоумышленников, банкам необходимо придерживаться следующих правил:

1. Генерировать пару ключей ЭЦП клиента и хранить секретный ключ должен только клиент. Сотрудники и представители банка не должны иметь доступа к секретному ключу ЭЦП клиента. В этом случае вся ответственность по сохранности и компрометации секретного ключа ЭЦП лежит всецело на клиенте.
2. Договор на обслуживание и сертификаты открытых ключей ЭЦП клиентов принимаются банком следующим образом:
 - по почте или любой доставке в банк – с нотариальным заверением факта подписи руководителя организации под Договором и Сертификатом открытого ключа ЭЦП;
 - при личном посещении банка руководителем, с подписью в присутствии ответственного сотрудника банка.

Все остальные варианты таят в себе угрозу подделки печатей и подписей руководителя.

3. Необходимо проинформировать клиентов банка о том, что подключение к электронному банкингу необходимо осуществлять через защищенный вспомогательный Web-сервер системы iBank 2 UA (<https://ibank.bankname.com>)

Допустимо использование клиентом ссылки, ранее сохраненной в своем Web-браузере ("Закладки"). В любом случае клиент обязан контролировать соответствие URL точки входа тому URL, который будет отображаться в его Web-браузере. Если клиент заходил на <https://ibank.bankname.com>, но потом произошло перенаправление на <http://www.bankname.com/ibank> (основной Web-сайт банка), то это **недопустимая ситуация**. Никаких перенаправлений быть не должно.

При эксплуатации системы iBank 2 UA практически всегда банк имеет два Web-ресурса – основной Web-сайт банка (<http://www.bankname.com>) и защищенный вспомогательный Web-сервер системы iBank 2 UA (<https://ibank.bankname.com>).

На основном Web-сайте банка расположена вся информация о банке, об услугах, тарифах и пр. Среди этой информации всегда есть упоминание наличия в банке системы электронного банкинга. И очень часто присутствуют ссылки на вход в систему iBank 2 UA.

Такая ситуация опасна с точки зрения безопасности системы. Клиенты привыкают подключаться к системе iBank 2 UA через незащищенный основной Web-сайт банка. Даже если потом сценарий предполагает переход клиента на защищенный Web-сервера системы iBank 2 UA и последующую загрузку стартовых HTML-страниц, конфигурационных XML-файлов и Java-апплетов с защищенного вспомогательного Web-сервера iBank 2 UA, тем не менее в этом случае появляется возможность для нанесения атаки на клиента со стороны злоумышленников.

Для исключения угроз по подмене ресурсов банкам необходимо придерживаться следующих правил:

1. **Защищенный Web-сервер системы iBank 2 UA.** Необходимо обеспечить жесткий контроль доступа к обновлению данных на защищенном вспомогательном Web-сервере iBank 2 UA. Должен быть четко определен круг сотрудников, которые имеют право редактировать данные на вспомогательном защищенном Web-сервере iBank 2 UA. Недопустимо наличие других приложений на серверах iBank 2 UA. Ошибки в администрировании сторонних приложений, установленных на серверах iBank 2 UA, ставят под угрозу всех клиентов, работающих по системе электронного банкинга. На защищенном Web-сервере системы iBank 2 UA должны размещаться:

- главная HTML-страница ;
- информация об услугах электронного банкинга;
- стартовые HTML-страницы для онлайн-овых АРМов;
- клиентские дистрибутивы;
- системное ПО для клиентов (Sun Java Plugin, патчи к Web-браузерам);
- документация для клиентов.

На HTML-страничках защищенного Web-сервера системы iBank 2 UA допустимо использование одной единой ссылки на основной Web-сайт банка. Недопустимо размещение на HTML-страницах динамических блоков (баннеры, новости и пр.) с внешними ссылками, которые загружаются с любых других ресурсов, кроме защищенного Web-сервера системы iBank 2 UA. Если банк вместо встроенного защищенного Web-сервера системы iBank 2 UA использует промышленный Web-сервер (Apache, IIS и др.), то необходимо своевременно проводить обновления (патчи), связанные с найденными уязвимостями промышленных Web-серверов.

2. **SSL-сертификат.** Обязательным является получение банками полноценных валидных SSL-сертификатов у мировых Удостоверяющих Центров - Thawte, VeriSign и др. Подробно о приобретении SSL-сертификата можно ознакомиться в документе **Инструкция по получению SSL-сертификата.**

Банкам, использующим полноценные валидные SSL-сертификаты, изданные мировыми Удостоверяющими Центрами (Thawte, VeriSign), целесообразно размещать на защищенном Web-сервере системы iBank 2 UA баннер-ссылку для проверки SSL-сертификата банка в Удостоверяющем Центре.

Банкам, использующим самозаверенные SSL-сертификаты, настоятельно рекомендуется:

- либо получить полноценный валидный SSL-сертификат в мировом Удостоверяющем Центре;

- либо использовать самозаверенный SSL-сертификат с обязательной раздачей на дискете клиентам и последующей установкой этого сертификата в Web-браузеры клиентов.
3. **Основной Web-сайт банка.** Доступ к управлению основным Web-сайтом банка должен быть **строго ограничен**. Особенно это касается административных полномочий. Часто банки заказывают свои Web-сайты у сторонних разработчиков. В рамках создания и сопровождения сайта предоставляют стороннему разработчику административный доступ к основному Web-сайту банка. Подобный подход с внешним (из Интернета) администраторским доступом к основному Web-сайту банка категорически **недопустим**. Доступ к редактированию данных должен быть строго ограничен. Как средствами CMS (система управления контентом, как правило, поставляется разработчиком сайта), так и средствами системного ПО.

На основном Web-сайте банка в разделе об услугах электронного банкинга должно быть указано, что вся информация об услугах и точка входа расположены на отдельном защищенном Web-сервере. Также должна быть в явном виде указана ссылка на защищенный Web-сервер – <https://ibank.bankname.com>.

4. Обеспечение целостности Web-серверов.

Банкам настоятельно рекомендуется организовать внутри банка внешним приложением контроль целостности файлов, расположенных на защищенном вспомогательном Web-сервере (периодическая загрузка по https всех файлов с защищенного Web-сервера, расчет и сравнение хеш-функций под файлами).

Рекомендации клиентам

В общем случае похитить у клиентов секретные ключи ЭЦП с паролями можно несколькими путями. Два основных:

- Создание и установка клиенту вредоносного программного кода – "трояна", настроенного исключительно на похищения паролей и секретных ключей ЭЦП клиентов для конкретной системы электронного банкинга (в том числе и iBank 2 UA);
- Психологические (социальные) методы. Например, рассылка писем по электронной почте от имени службы техподдержки банка с просьбой зайти по указанной в письме ссылке и проверить правильность работы новой версии системы.

В связи с этим клиенту необходимо иметь хотя бы общее представление о "троянах". Борьба с "троянами" невозможна. Если специализированный "троян" установлен клиенту, то вся среда исполнения программ полностью дискредитирована. Нужно переустанавливать ОС и системное ПО из доверенного источника. Выявить внешними антивирусными средствами специализированный и малораспространенный "троян" чрезвычайно сложно и дорого. Единственный способ борьбы с вредоносными программными кодами – это превентивные меры, обеспечение максимально защищенной среды исполнения на компьютере клиента. В этой связи клиентам необходимо придерживаться следующих правил:

- устанавливать ОС и системное ПО только из доверенных источников;
- постоянно отслеживать и устанавливать все патчи к ОС и системному ПО только из доверенных источников;

- постоянно отслеживать и устанавливать все патчи к Web-браузеру и виртуальной Java-машине только из доверенных источников;
- использовать персональные файрволы в максимально жестком режиме;
- использовать и постоянно обновлять антивирусные средства.

Клиентам категорически не рекомендуется скачивать и устанавливать непроверенное ПО, открывать непроверенные приложения к письмам (особенно от неизвестных отправителей).

Глава 6

Источники дополнительной информации

С дополнительной информацией по данной тематике можно ознакомиться в следующих документах:

- *Общая информация о системе iBank 2 UA*
- *Инструкция по получению SSL-сертификата*
- *Файловая структура Сервера Приложения iBank 2 UA*
- *Установка системы iBank 2 UA под ОС Windows/Unix*
- *Процессы управления сотрудниками банка и клиентами в системе iBank 2 UA*
- *Юридичне обґрунтування застосування електронних документів, створення та використання систем «клієнт-банк», зокрема системи «iBank 2 UA»*

Примечание: _____

Со всеми предложениями и пожеланиями по документации обращайтесь по электронному адресу support@bifit.com.ua
