Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

Политика безопасности функционирования системы дистанционного банковского обслуживания BS-Client v3

Студент: *Пупкова Елена Викторовна*
Группа: *115*
Курс: *«Защита информации»*

Листов 8
Москва, 2005

ОГЛАВЛЕНИЕ

1. Введение

Система дистанционного банковского обслуживания (ДБО) BS-Client предназначена для автоматизации расчетно-кассового обслуживания всех типов респондентов банка. Предоставляя возможность осуществления удаленного документооборота - обмена финансовыми документами – необходимо уделять повышенное внимание вопросам безопасности. В связи с этим была разработана политика безопасности, определяющая требования по обеспечению безопасности функционирования платежной системы (типа «Банк-Клиент»), используемой для управления банковскими счетами Организации. Финансовые документы вводятся на автоматизированном рабочем месте (АРМ) Клиента, подписываются электронными подписями, зашифровываются и отправляются в банк по каналам связи. Система BS-Client позволяет также принимать выписки из банка о состоянии счетов и произведенных финансовых операциях по счетам.

2. Основные положения политики безопасности

- Автоматизированная система (далее АС) BS-Client должна обеспечить целостность передаваемых данных и их конфиденциальность;
- АС BS-Client должна обеспечить сохранение юридической значимости документов, что достигается применением электронно-цифровой подписи (ЭЦП);
- Все документы должны шифроваться перед передачей по каналам связи;
- В АС BS-Client предусмотрен механизм разграничения доступа к конфиденциальной информации;
- АС BS-Client обеспечивает ведение электронных журналов регистрации, содержащих полную информацию о всех созданных, переданных и принятых документах у операционистов банка, на коммуникационном сервере и у клиентов;
- В АС BS-Client осуществляется периодическое архивирование всей информации в зашифрованном виде, исключающем несанкционированный доступ.

3. Типы криптографических преобразований

В системе BS-Client используется криптографические стойкие шифрование и электронно-цифровая подпись (ЭЦП) всех данных, которыми Клиенты обмениваются с Банком на основе различных ключевых носителей (Excellence, CryptoPro CSP, Crypto COM, LanCrypto, Message-PRO, Open SSLCrypto-C). Шифрование защищает данные от перехвата злоумышленником, ЭЦП однозначно удостоверяет авторство данных. В зависимости от выбранного ключевого носителя могут использоваться различные алгоритмы подписи (ГОСТ Р34.10-94, RSA), шифрования (ГОСТ 28147-89) и хеширования (ГОСТ, SHA1, MD2, MD5).

При личной встрече Банк предоставляет Клиенту один или несколько ключевых комплектов. Каждый комплект состоит из секретного ключа и сертификата (открытого ключа) Клиента и сертификата (открытого ключа) Банка. Все электронные документы, передаваемые или получаемые из Банка по системе BS-Client, шифруются и подписываются этими ключами.

Каждый передаваемый в Банк документ подписывается требуемым количеством (1 или 2) электронно-цифровых подписей. При приеме документа Банк проверяет верность электронных подписей.

По умолчанию параметры использования и перегенерации ключей в системе BS-Client определяются автоматически. Предусмотрена возможность выбора каждым абонентом желательных для него алгоритмов подписи и ключевого обмена, а также длин соответствующих ключей, из числа реализованных в системе. Распознавание используемых алгоритмов в системе BS-Client происходит автоматически.

Система BS-Client для защиты информации использует различные средства криптозащиты информации (СКЗИ), при работе которых для реализации задач формирования/проверки цифровой подписи и шифрации/расшифровки данных используются так называемые ключевые пары, состоящие из двух связанных между собой ключей: открытого и секретного.

Секретный ключ (файл секретного ключа, либо ключ, записанный на специальный ключевой носитель) является конфиденциальной информацией. Защита данного ключа от несанкционированного копирования лежит на владельце ключа.

Секретный ключ в большинстве современных СКЗИ распространяется в виде сертификата. Сертификат представляет собой открытый ключ, заверенный цифровой подписью центра сертификации (ЦС) – специального органа, в функции которого входит выдача сертификатов. Подразумевается, что все участники ключевого обмена «доверяют» ЦС. Открытый ключ не является конфиденциальной информацией и может распространяться по открытым каналам связи без дополнительной защиты.

Каждая ключевая пара, используемая в системе, характеризуется уникальным идентификатором – UIDом.

Ключевая пара может создаваться в банке (если установлен Центр Авторизации) или выдаваться в готовом виде. Сертификат как правило имеет срок годности, но может также быть бессрочным. Срок годности сертификата определяется автоматически при установке сертификата.

Для выполнения различных операций криптографических преобразований используются различные части ключевой пары:

№	Наименование операции	Используемые ключи
1.	Формирование цифровой подписи	Секретный ключ подписывающего абонента
2.	Проверка цифровой подписи	Открытый ключ (сертификат) подписавшего абонента
3.	Шифрация данных	Открытый ключ (сертификат) получателя шифрованных данных
4.	Расшифровка данных	Секретный ключ абонента, получившего зашифрованные данные

3.1. Поддерживаемые типы средств криптозащиты информации (СКЗИ)

Система BS-Client поддерживает следующие типы систем криптозащиты информации:

- Excellence/4.0
- LAN Crypto/2.35
- Message-PRO 1.1
- M-Pro v1.34 (GOST PSE)
- M-Pro v2.x
- CryptoPro CSP/1.1
- Verba-OW/4
- Crypto COM/2.2

- Open SSL
- Crypto-C

Каждая СКЗИ характеризуется списком параметров по умолчанию:

- **Поддержка шифрации на старых ключах -** осуществляется поддержка шифрации данных старыми открытыми ключами абонента;
- **Поддержка дешифрации старых ключей -** поддержка дешифрации данных, зашифрованных собственными старыми открытыми ключами; этим свойством обладают криптобиблиотеки Excellence/4.0 и LAN Crypto/2.35;
- **Поддержка удаленной перегенерации ключей -** под удаленной перегенерацией ключей следует понимать операцию обновления рабочих ключей Клиента; необходимость в обновлении ключей может возникнуть в нескольких случаях:
  1. после установки и настройки BS-Client для обновления регистрационного ключа и сертификата ограниченного периода действия;
  2. при плановой смене ключей в связи с приближающимся истечением периода действия текущего рабочего сертификата;
  3. в любой момент по желанию Клиента.

  этим свойством обладают криптобиблиотеки Excellence/4.0, LAN Crypto/2.35, Message-PRO 1.1, M-Pro v1.34 (GOST PSE), M-Pro v2.x, CryptoPro CSP/1.1, Crypto COM/2.2, Open SSL и Crypto-C;
- **Алгоритм перегенерации ключей -** выбирается из списка возможных значений:
  1. Генерация открытого ключа пользователем – открытый ключ и сертификат генерируются на клиентском месте без участия Центра сертификации (ЦС). Этим свойством обладают криптобиблиотеки Excellence/4.0, LAN Crypto/2.35.
  2. Генерация открытого ключа в ЦС – на клиентском месте генерируется запрос в ЦС на новый сертификат, а ЦС по этому запросу выдает клиенту новый сертификат. Этим свойством обладают криптобиблиотеки Message-PRO 1.1, M-Pro v1.34 (GOST PSE), M-Pro v2.x, CryptoPro CSP/1.1, Crypto COM/2.2, Open SSL и Crypto-C.

3.2. Подпись документов

Цифровая подпись применяется для контроля целостности данных и подтверждения авторства их подписавшего. Подпись налагается только на незашифрованные данные. Документ может быть подписан одной или двумя подписями.

Система BS-Client позволяет выполнять процедуру подписи документов в зависимости от настроенных параметров (криптографический профиль пользователя системы, параметры документа и пр.).

Пользователь обязательно должен иметь доступ к секретному ключу, с помощью которого выполняется процедура подписи документов.

3.3. Проверка подписи документов

Проверка цифровой подписи может быть осуществлена любым абонентом, имеющим доступ к открытому ключу подписавшего абонента. При проверке подписи определяется: кто и когда подписал данные, искажены они или нет.

Для выполнения проверки подписи документов исходными параметрами являются:

1. Криптографический профиль пользователя системы
2. Тип криптобиблиотеки, с помощью которой подписан документ
3. Количество подписей под документом

3.4.Подпись пакетов

Подпись транспортных пакетов производится автоматически, если данный сервис активирован в настройках профиля подписывающего абонента.

Подпись транспортного пакета осуществляется секретным ключом подписывающего абонента. Если для подписи документов могут быть использованы несколько ключей абонента, то подпись транспортного пакета осуществляется первым из списка возможных ключей.

Для выполнения подписи транспортного пакета исходными параметрами являются:

1. Криптографический профиль пользователя системы
2. Идентификатор ключевой пара (UID) абонента, которому отправляются данные.

3.5.Проверка подписи пакетов

Проверка цифровой подписи транспортных пакетов производится автоматически, если данный сервис активирован в настройках профиля абонента, получившего данные.

Проверка цифровой подписи может быть осуществлена любым абонентом, имеющим доступ к открытому ключу подписавшего абонента.

При проверке подписи определяется: кто и когда подписал данные, искажены они или нет.

Для выполнения проверки подписи исходными параметрами являются:

1. Криптографический профиль пользователя системы
2. Тип криптобиблиотеки, с помощью которой подписан пакет.

Схематическое изображение выполнения функций подписи и шифрации транспортных пакетов показано на Рис. 1

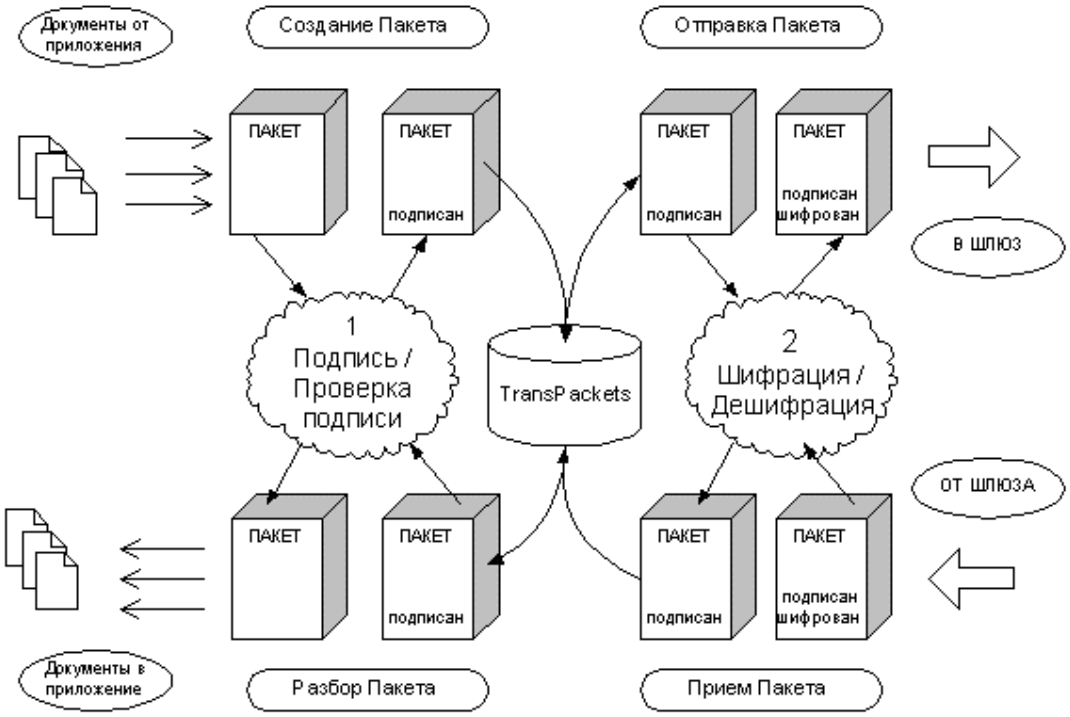

Рис. 1. Выполнение в ядре функций шифрации/дешифрации транспортных пакетов

3.6. Шифрование пакетов

Шифрование данных применяется с целью исключения несанкционированного ознакомления с ними при их хранении и передаче по каналам связи.

Для сокращения объема зашифрованных данных в системе предусмотрена возможность их предварительного сжатия с помощью встроенного архиватора. Данные после шифрования сжать нельзя.

Шифрование данных осуществляется по алгоритму соответствующей криптобиблиотеки. Например, при работе с криптобиблиотекой Excellence шифрование данных осуществляется в соответствии с режимом гаммирования с обратной связью ГОСТ 28147-89. Алгоритм ключевого обмена и используемая длина ключа для каждого пользователя выбирается перед генерацией новых ключей.

Шифрование данных выполняется открытым ключом (сертификатом) получателя шифрованных данных.

Для выполнения шифрации исходными параметрами являются:

1. Криптографический профиль пользователя системы
2. Тип криптобиблиотеки, с помощью которой подписан пакет
3. Идентификатор ключевой пары (UID) абонента, для какого шифруются данные.

3.7. Расшифрование пакетов

Расшифровка транспортных пакетов производится автоматически.

Распаковка данных, если они были сжаты, при расшифровке транспортных пакетов происходит автоматически. При расшифровке данных сначала определяется возможность доступа к ним, потом данные расшифровываются по алгоритму соответствующей криптобиблиотеки. Осуществляется контроль целостности данных.

Для расшифровки транспортных пакетов используется секретный ключ абонента, получившего зашифрованные данные.

Для выполнения дешифрации исходными параметрами являются:

1. Криптографический профиль пользователя системы
2. Тип криптобиблиотеки, с помощью которой зашифрован пакет.

3.8. Обработка входящих пакетов, содержащих ошибки

«Плохой» пакет сохраняется в базе данных принимающей стороны. Входящий пакет признается плохим, если не проходит хотя бы одну из следующих проверок:

1. Размер пакета (реальный размер пакета сравнивается со значением, прописанным в шапке)
2. Контрольная сумма
3. Корректная дешифрация (если задано)
4. Номер лицензии отправителя
5. Номер лицензии получателя (сравнивается с собственным номером).

4. Обмен открытой ключевой информацией

Необходимость в обмене открытыми ключами (сертификатами) в системе BS-Client возникает в следующих случаях:

1. При обновлении ключей Клиента;
2. При смене ключей банковского администратора;
3. При появлении новых ключей сертификационного центра.

Под обновлением ключей Клиента следует понимать операцию перегенерации ключей Клиента на его рабочем месте. В зависимости от типа СКЗИ процедура перегенерации ключей осуществляется по-разному. Для ключей Message-PRO 1.1, M-Pro v1.34 (GOST PSE), M-Pro v2.x, CryptoPro CSP/1.1, Open SSL, Crypto-C запрос на перегенерацию сертификата инициируется на Клиенте и по даставке в Банк выгружается в файл для ЦС. Полученный в ЦС сертификат доставляется Клиенту. Для ключей Excellence/4.0, LAN Crypto/2.35 перегенерация осуществляется встроенным сервисом BS-Client.

В случае возникновения необходимости перехода на новые ключи Банка, новый сертификат (банковский открытый ключ) передается всем абонентам посредством встроенного сервиса системы BS-Client.

В случае смены рабочего сертификата центра сертификации (при работе с ключами Message-PRO 1.1, M-Pro v1.34 (GOST PSE), M-Pro v2.x, CryptoPro CSP/1.1 или Open SSL) пересылка нового сертификата ЦС осуществляется посредством встроенного сервиса системы BS-Client

Примечание: При смене ключей клиента, банка или сертификационного центра старые ключи не заменяются новыми, а просто блокируются.

СПИСОК ЛИТЕРАТУРЫ

1. Системная и эксплуатационная документация по системе ДБО BS-Client:
   - ✓ «ДБО BS-Client v.3.0. Сервер ДБО. Справочник администратора Банка»
   - ✓ «ДБО BS-Client v.3.0. Подсистема Банк-Клиент. Руководство администратора Клиента»
   - ✓ «ДБО BS-Client v.3.0. Подсистема Интернет-Клиент. Руководство по установке удаленного АРМ»
2. Материалы официального сайта компании Bank's Soft Systems.