Аппаратная криптография. Особенности «тонкой» настройки

С. В. Конявская, *к. ф. н.,*
Д. Ю. Счастный,
Т. М. Борисова
ЗАО «ОКБ САПР»

Логика защиты

Сегодня терминальные решения и криптографическая защита являются безусловными лидерами рейтинга явлений, формирующих «картину мира» информационной безопасности. Однако именно эти два лидера на сегодняшний день достаточно проблематично сочетаются в одной информационной системе.

При внедрении в систему терминального доступа (СТД) системы криптографической защиты информации (СКЗИ) возможно возникновение ряда проблем.

1. СКЗИ может не предусматривать возможности работы в режиме терминального доступа вообще, поскольку не поддерживает процедуры удаленных криптографических преобразований.

2. Если ключи пользователя хранятся на терминальном сервере (ТС), то они вообще, строго говоря, не являются *ключами пользователя*, и подпись, выполненная с их помощью, никак не подтверждает авторство последнего.

3. Если ключи находятся на стороне терминального клиента (ТК), а выработка ЭЦП выполняется на стороне ТС, а не на стороне пользователя, который находится на ТК, то закрытые ключи ключевых пар передаются в рамках терминальной сессии по сети. Такая подпись тоже не может вполне гарантировать авторство.

4. В значительном числе случаев, даже при выработке ЭЦП непосредственно на клиенте, в терминальном режиме необходима передача информационных наборов данных по сети. При передаче обработанных на стороне ТС данных (например, после вычисления от этих данных функции хэширования) пользователь, находящийся на стороне ТК, не может быть уверен в их корректности. Они могли быть изменены при передаче по сети до вычисления функции хеширования, или функция хеширования могла быть вычислена не от переданных данных, или переданный корректный хэш мог быть подменен «на обратном пути».

5. Даже в случае, когда все вычисления производятся на стороне ТК, во время вычислений закрытый ключ ключевой пары может загружаться в оперативную память ТК либо же оставаться на ТК для долговременного хранения. При том что терминальные клиенты, как правило, защищены менее тщательно, чем терминальные серверы, это означает, что закрытый ключ может быть несанкционированно скопирован и использован в корыстных целях.

Таким образом, система криптографической защиты информации при работе в условиях терминального доступа должна удовлетворять следующим условиям:

- СКЗИ должна поддерживать работу в терминальном режиме (требование 1);

- закрытый ключ ключевой пары ЭЦП должен располагаться на ТК (требование 2);
- информационные наборы данных должны создаваться на ТК (требование 3);
- выработка подписи и шифрование данных должны производиться на ТК (требование 4);
- должно быть исключено несанкционированное использование закрытого ключа ключевой пары в период его применения или хранения на ТК (требование 5).

В настоящее время реализованы и внедряются СКЗИ, построенные в строгом соответствии с этими требованиями. В качестве примера опишем систему, построенную на базе программной отечественной СКЗИ и аппаратного отечественного персонального средства криптографической защиты информации (ПСКЗИ). Оба средства сертифицированы.

ПСКЗИ поддерживает операции удаленных криптографических преобразований, поэтому построенная на его основе система удовлетворяет требованию 1.

Вся работа с закрытым ключом ключевой пары производится внутри ПСКЗИ, которое подключается к терминальному клиенту, что удовлетворяет требованиям 2 и 3.

ПСКЗИ аппаратно реализует все российские криптографические алгоритмы и осуществляющее безопасное хранение закрытых ключей ключевых пар в памяти устройства. То есть все криптографические операции выполняются в доверенной среде, и закрытый ключ ключевой пары никогда не покидает самого устройства и не попадает в оперативную память терминального клиента, что при построении надежной системы PKI позволяет обеспечить требования 4 и 5.

В качестве терминальных клиентов, используемых в системе терминального доступа, с описываемой системой могут выступать клиенты под управлением следующих операционных систем (для которых реализовано терминальное программное обеспечение для ПСКЗИ):

- Win32 (Windows 98, Windows 2000, Windows XP);
- WinCE;
- Linux (на примере «Ками-терминала»).

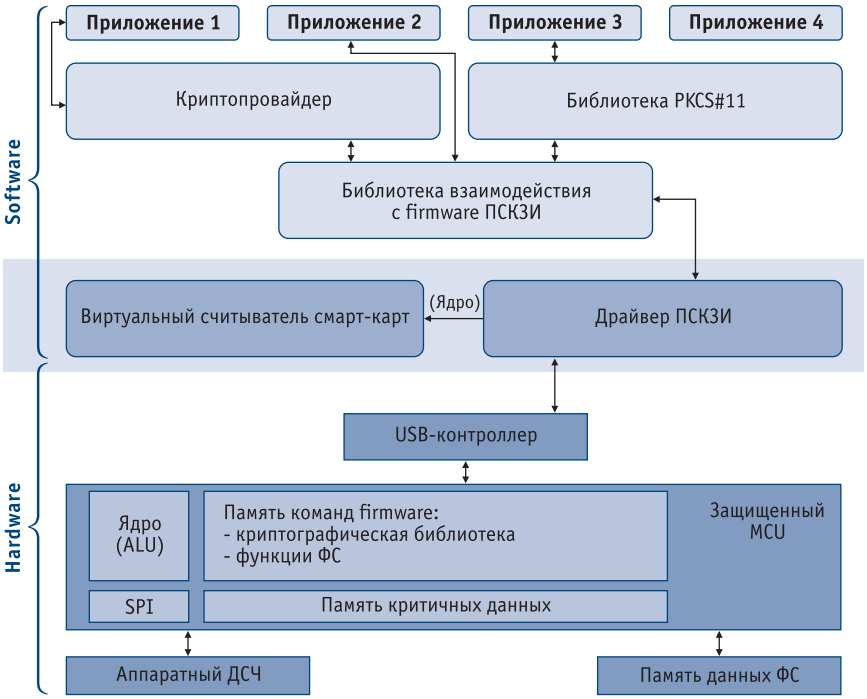

Рис. 1. ***Архитектура ПСКЗИ***

Поддержка различных терминальных ОС позволяет применять тонкие клиенты разных производителей и моделей (Wyse, Ками, Depo и многие другие), что предоставляет определенную свободу действий заказчику, внедряющему решение. Терминальные серверы могут работать как под управлением Windows, так и под управлением Citrix.

Технология защиты

Функциональность ПО аппаратного ПСКЗИ (терминальное применение)

Корректное применение ПСКЗИ для криптографической защиты электронных сообщений и документов при использовании технологий терминального доступа возможно в силу следующих причин:

- ключевая информация, ассоциированная с пользователем, и программное обеспечение, выполняющее криптографические преобразования, сосредоточены в одном устройстве, доступны на исполнение только авторизованному пользователю и технологически защищены от несанкционированного чтения и модификации;
- собственные ресурсы (возможность получения аппаратной случайной последовательности, возможность хранения собственного закрытого и открытого ключей, возможность хранения отрытого ключа терминального сервера, а также возможность вычисления и проверки подписи) для организации защиты виртуальных каналов, построенных в рамках протоколов RDP или ICA;
- поддержка стандартных интерфейсов (криптопровайдера и PKCS#11), позволяющая избавить производителей ПО, взаимодействующего с внутренним ПО ПСКЗИ, от изучения особенностей реализации процедур этого взаимодействия.

Схема взаимодействия аппаратных и программных компонентов ПСКЗИ представлена на рис. 1.

Выполнение криптографических операций

Все криптографические преобразования выполняются непосредственно в устройстве. Код, реализующий криптографические алгоритмы, содержится в ПСКЗИ и технологически защищен от несанкционированного изменения.

Ключи, необходимые для проведения криптографических расчетов, также хранятся в устройстве, где и генерируются с использованием аппаратного ДСЧ. Хранятся ключи в фай-

ловой системе ПСКЗИ в защищенном виде, поэтому несанкционированный доступ к ним путем извлечения и прямого чтения микросхем, которые используются для хранения файлов, исключен. Еще одной особенностью ключевых файлов является регламент доступа: несмотря на то что ключевые файлы – объекты файловой системы, работать с ними как с обычными файлами нельзя. Firmware ПСКЗИ спроектировано таким образом, что с ключевыми файлами можно работать только из функций криптографических преобразований, и никак иначе. В свою очередь, функции криптографических преобразований получают доступ к ключевым файлам только после того, как пользователь пройдет процедуру аутентификации и подтвердит с помощью PIN-кода, что он имеет право доступа к ключевым данным, хранящимся в ПСКЗИ.

Итак, можно утверждать, что в случае применения персонального средства криптографической защиты информации для криптографических преобразований в терминальном режиме:

- ключ не покидает устройство;
- данные для вычисления значения хэш-функции проходят через устройство;
- вычисление ЭЦП и шифрование происходит в устройстве;
- ключ не появляется в оперативной памяти компьютера;
- НСД к ключу технологически невозможен ни при его генерации, ни в процессе работы устройства, ни во время его хранения в устройстве.

Модель передачи данных через виртуальные каналы

Использование стандартного ПО ПСКЗИ в терминальном сеансе приводит к следующему результату: пользователь запускает программу на терминальном сервере, программа через интерфейс CryptoAPI (CSP) или PKCS#11 обращается к библиотеке взаимодействия с firmware ПСКЗИ, которая, в свою очередь, обращается к драйверу устройства для обмена данными с устройством. Однако операционная система автоматически не перенаправляет обращения из терминальной сессии к устройству, установленному на терминале, и обращения идут к устройству, установленному в сервере. Операционная система терминального сервера в рамках терминальной сессии автоматически предоставляет пользователю возможность работы только с локальной мышью, клавиатурой и дисплеем, а доступ к остальному периферийному оборудованию необходимо организовывать специальным образом.

Известно, что взаимодействие ПО терминального сервера ОС Windows (Windows 2000 Advanced Server, Windows 2003) с клиентом происходит в рамках специального протокола – remote desktop protocol (RDP). В рамках этого протокола от пользователя на сервер передаются нажатия на клавиши и движения мыши на терминальном клиенте, а от сервера передается изображение виртуального экрана. С точки зрения пользователя терминального клиента, взаимодействие с сервером под управлением Citrix XenApp (Presentation Server) ничем не отличается от работы с терминальным сервером под управлением Windows, тогда как на самом деле то же самое взаимодействие клиента и сервера здесь протекает по протоколу independent computing architecture (ICA), который отличается от протокола RDP.

Но оба эти протокола предоставляют возможность построения так называемых виртуальных каналов.

Виртуальный канал – это последовательность логических соединений между посылающим и принимающим компьютерами. Соединение считается установленным, если оба компьютера обменялись служебной информацией и подтвердили параметры связи.

С точки зрения прикладного программного обеспечения, выполняющегося на терминальном сервере в рамках терминальной сессии, виртуальные каналы обеспечивают передачу данных между сервером и клиентом независимо от протоколов транспортного уровня (TCP/IP, IPX) и сами, в свою очередь, являются некоторым подобием реализации протоколов транспортного уровня. Для построения виртуального канала необходимо реализовать серверную компоненту на терминальном сервере и клиентскую компоненту на стороне терминального клиента. Если зарегистрировать клиентскую компоненту на ТК, то прикладное программное обеспечение, выполняясь на ТС, получит возможность обмениваться данными непосредственно с терминальными клиентами.

Таким образом, для использования ПО ПСКЗИ в терминальном режиме в структуру, которая описанна на рис. 1, необходимо внести изменения. Библиотека взаимодействия с firmware ПСКЗИ на терминальном сервере должна обращаться не к драйверу устройства на сервере, а к библиотеке взаимодействия с firmware ПСКЗИ на ТК, которая, в свою очередь, будет обращаться к устройству на ТК через соответствующий драйвер.

Функционально в библиотеке взаимодействия с firmware ПСКЗИ можно выделить три основные группы функций:

- функции работы с устройством как с объектом операционной системы;
- функции нотификации (извещения о фактах установки и удаления устройства);
- функции обмена командами и данными с устройством.

Соответственно, эти три группы функций необходимо реализовать и на ТС, и на ТК. Причем серверная компонента не зависит от операционной системы ТК, так как виртуальные каналы обеспечивают унифицированный интерфейс взаимодействия с ТК (рис. 2).

Реализация серверной компоненты

Серверная компонента представляет собой динамически загружаемую библиотеку, экспортирующую необходимые функции. Библиотека взаимодействия с firmware ПСКЗИ во время старта определяет режим работы (локально, в терминальной сессии Windows Terminal Server, в терминальной сессии Citrix) и загружает нужную библиотеку. Та, в свою очередь, создает виртуальные каналы, в рамках которых производится весь последующий обмен данными между приложениями, запускаемы-

ми в терминальной сессии и обращающимися к ПСКЗИ, и ПСКЗИ, установленными на терминале.

Реализация клиентской компоненты

Клиентская компонента для Win32

Клиентская компонента для Win32 (Windows 98, Windows 2000, Windows XP) обеспечивает обработку команд обмена данными с устройствами. В момент создания терминальной сессии происходит инициализация библиотек и создание виртуальных каналов с терминальным сервером. После этого библиотеки обрабатывают запросы от серверной компоненты и транслируют их через библиотеку взаимодействия с firmware ПСКЗИ на терминале в устройство или сообщают о фактах установки/удаления ПСКЗИ из терминала (рис. 3).

Клиентская компонента для WinCE

Windows CE (она же WinCE) – это вариант операционной системы Microsoft Windows для наладонных компьютеров, мобильных телефонов и встраиваемых систем. Поддерживаются архитектуры x86, MIPS, ARM и процессоры Hitachi SuperH. Windows CE оптимизирована для устройств, имеющих минимальный объем памяти.

Одной из особенностей Windows CE является то, что в большинстве случаев операционная система, загружаемая на конкретном устройстве, не может быть расширена дополнительным функционалом. Таким образом, для функционирования клиентской компоненты необходимо на этапе подготовки образа операционной системы включить в него клиент RDP или Citrix ICA, а также необходимые библиотеки.

В остальном клиентская компонента для Windows CE полностью аналогична по своему составу и зависимостям клиентской компоненте для Win32 (см. рис. 3).

Клиентская компонента для «Ками-терминал»

«Ками-терминал» – это дистрибутив ОС Linux, предназначенный специально для использования на терминальных клиентах.

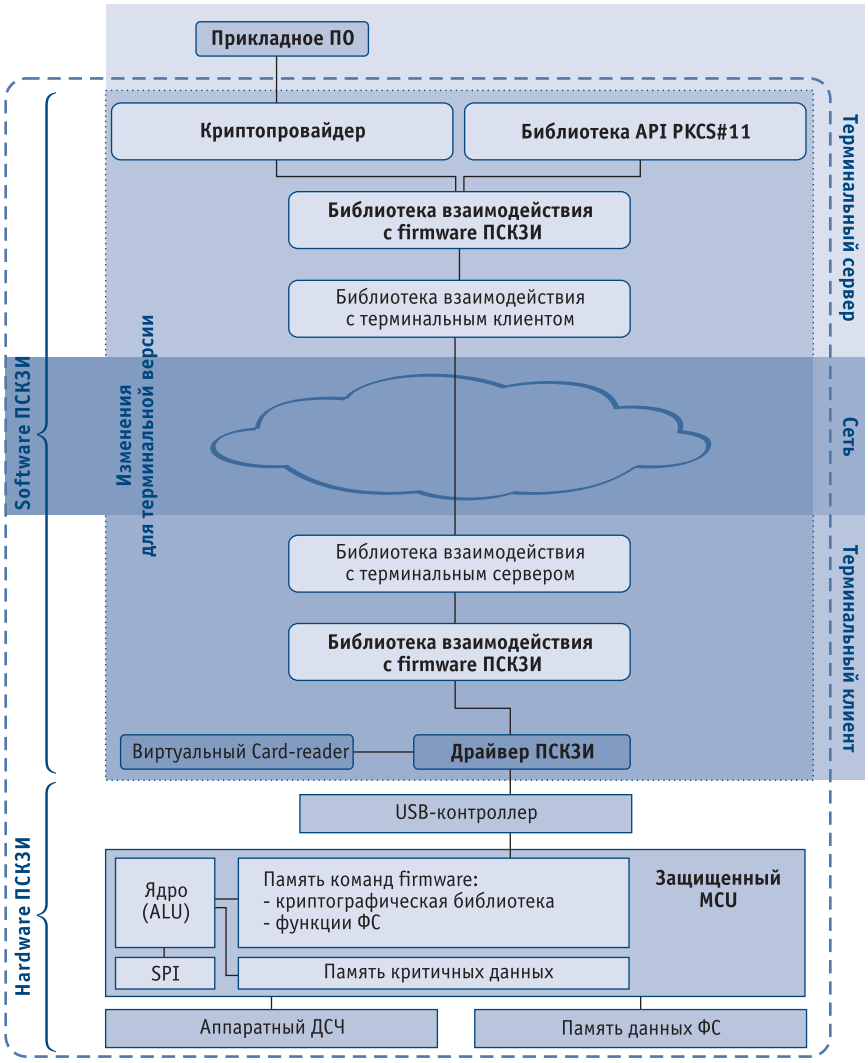

Рис. 2. ***Взаимодействие приложения с ПСКЗИ в терминальном сеансе***

Загрузка «Ками-терминала» проходит в четыре этапа.

1. *Загрузка базового образа файловой системы (ФС).* С заранее подготовленного носителя стартует базовая часть, состоящая из ядра Линукс и образа ФС с минимальным набором файлов, необходимых для установки сетевого соединения с сервером загрузки.

2. *Аутентификация и загрузка профиля пользователя.* Пользователю предлагается подключить ПСКЗИ и ввести PIN-код. При успешном завершении процесса аутентификации с устройства считывается профиль пользователя, на основе которого производится загрузка файла настроек и пакетов ПО с сервера загрузки.

3. *Загрузка, проверка и установка пакетов ПО, необходимых для старта сессии с ТС.* С сервера загрузки по протоколу NFS скачиваются пакеты ПО, указанные в файле настроек профиля пользователя на сервере. Для каждого загруженного пакета вычисляется хэш, значение которого сравнивается с соответствующим значением, записанным в профиль пользователя в устройстве. В случае успеш-

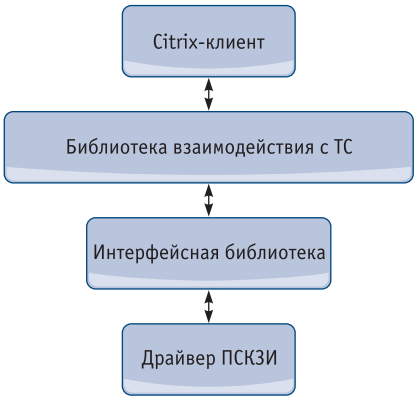

Рис. 3. ***Клиентская компонента ПСКЗИ***

НОВОСТИ

Cisco обновила интерактивный ресурс, посвященный ИБ

Начало своего нового, 2011 финансового года компания Cisco ознаменовала анонсом обновленной версии интернет-ресурса www.securityinitiativeadvisor.com, позволяющего заказчикам самостоятельно формировать стратегию обеспечения информационной безопасности в корпоративной сети.

За полтора года существования предыдущей версии web-ресурса у заказчиков появились новые задачи, а у Cisco - новые продукты. В связи с этим и возникла идея модернизации сайта.

Новый ресурс будет использоваться при консультировании клиентов как инструмент, позволяющий глубже понять структуру решений Cisco и сформировать целостное представление о том, как решать вопросы информационной безопасности во всей корпоративной сети. Сайт состоит из четырех разделов: «Оптимизация расходов», «Доступ из любой точки мира», «Развитие бизнеса» и «Соответствие нормативам». Каждый из них структурирован по конкретным темам. Так, в разделе «Соответствие нормативам» предусмотрено несколько категорий, раскрывающих вопросы идентификации, управления инцидентами, предотвращения краж информации и сегментации сети. В каждом подразделе клиентам предлагается пройти несложный опрос, после чего они получают рекомендации по обеспечению информационной безопасности (с конкретными примерами решения тех или иных задач) в соответствии с тем, что посетителя сайта интересует больше всего.

Перед компанией-заказчиком могут стоять различные задачи: расширение бизнеса, поглощение, снижение издержек, аудиторские проверки контролирующих органов, организация тесного взаимодействия с клиентами, партнерами и подрядчиками. В каждом конкретном случае новый ресурс поможет смоделировать комплексное решение, которое сможет обеспечить необходимый уровень защиты корпоративной сети в соответствии с требованиями завтрашнего дня.

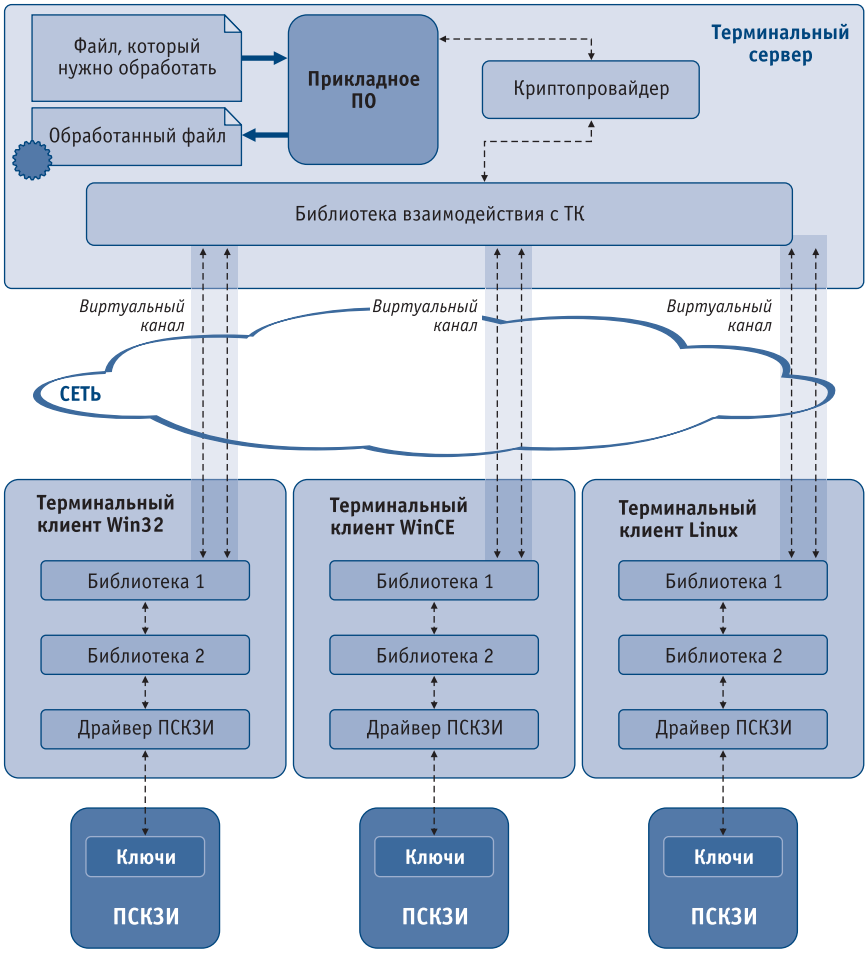

Рис. 4. ***Общая схема взаимодействия***

Примечание. «Библиотека 1» – библиотека взаимодействия с терминальным сервером, «Библиотека 2» – интерфейсная библиотека.

ного завершения проверки содержимое пакета устанавливается в ФС «Ками-терминала».

4. *Старт терминальной сессии.* На основе содержимого файла настроек устанавливается соединение с терминальным сервером и создаются виртуальные каналы.

Диаграмма зависимостей клиентской компоненты для Linux аналогична приведенной на рис. 3.

Что в результате?

Использование виртуальных каналов в терминальной сессии позволяет (независимо от типа используемого клиента) осуществлять обмен данными с ПСКЗИ, установленными в USB-слот терминала. Прикладное программное обеспечение и вызываемый им криптопровайдер продолжают работать в терминальной сессии точно так же, как и в локальном режиме. И хотя программы продолжают выполняться на терминальном сервере, обращения к устройствам перенаправляются на терминалы, в которые устройства и устанавливаются. В полученном варианте работы с терминальным сервером пользователь имеет возможность контролировать доступ к своему устройству и к ключам. То есть прикладное криптографическое ПО хранится и выполняется на терминальном сервере, а работа с ключами и информационными наборами осуществляется на терминале (рис. 4).

В данном случае взаимодействие прикладного ПО с ПСКЗИ производится через криптопровайдер, так как такова особенность взятого для примера прикладного ПО. Возможна реализация и с взаимодействием через PKCS#11. Этот вариант также реализован и применяется и, более того, имеет ряд преимуществ перед описанным. Однако этому будет посвящена отдельная статья. ■