Средства многофакторной аутентификации в современной инфраструктуре безопасности информационных систем

Multifactorial authentication media in modern infrastructure of information system security

Ключевые слова: многофакторный – multifactorial; аутентификация – authentication; программно-аппаратный комплекс – hardware and software system; сертификат – certificate.

В статье рассматривается многофакторный программно-аппаратный комплекс, позволяющий осуществлять аутентификацию с применением новейших сертификатов X509.

The article considers a multifactorial hardware and software system which allows to perform authentication based on the new X509 certificate.

КАРМАНОВ / KARMANOV A.
Андрей Геннадьевич
(office@itain.spb.ru)
кандидат технических наук, доцент,
ЗАО «Институт телекоммуникаций»,
Санкт-Петербург

Средства многофакторной аутентификации являются необходимым компонентом в инфраструктуре безопасности современных информационных систем. Растущие требования к защите информации от несанкционированного доступа приводят к необходимости разработки надежных и недорогих средств многофакторной аутентификации пользователей для различных приложений на основе цифровых сертификатов X509. Аутентификация с применением сертификатов является современной и надежной альтернативой использованию паролей не только при входе пользователей в домен, но также при работе с ресурсами, размещенными в сети.

Необходимо отметить, что аутентификация с применением сертификатов является альтернативой использованию паролей и представляется естественным решением в условиях, когда число пользователей сети велико (например – в Интернете). В таких обстоятельствах процедура предварительной регистрации пользователей, связанная с назначением и хранением их паролей, становится опасной, а иногда и просто нереализуемой. При использовании сертификатов сеть, которая дает пользователю доступ к своим ресурсам, не хранит информации о своих пользователях – они ее предоставляют сами в своих запросах в виде сертификатов, удостоверяющих личность пользователей. Сертификаты выдаются специальными уполномоченными организациями – центрами сертификации. Поэтому задача хранения закрытых ключей возлагается на самих пользователей, что делает это решение более масштабируемым, чем вариант с использованием паролей.

Большинство существующих решений на рынке имеет те или иные выраженные недостатки: проблемы совместимости или удобства использования, устаревшую и сложную при внедрении архитектуру, а во многих случаях такие решения могут быть необоснованно дорогими. Предлагается современный программно-аппаратный комплекс средств многофакторной аутентификации для систем Windows XP / Windows Server 2003 / Windows Vista на базе электронных ключей для шины USB, рассчитанный на применение, как в государственных, так и в коммерческих организациях.

ИНФРАСТРУКТУРА ПОДДЕРЖКИ СМАРТ-КАРТ В ОС WINDOWS

Операционные системы семейства Microsoft Windows обеспечивают встроенную поддержку использования смарт-карт и электронных ключей в различных приложениях. Традиционно обеспечение совместимости с конкретным типом смарт-карт или электронных ключей обеспечивалось разработкой специализированного крипто-сервис-провайдера для смарт-карт, который выполняет роль посредника между операционной системой и смарт-картой либо электронным ключом. Такая схема взаимодействия используется практически во всех решениях, представленных на российском рынке компаниями

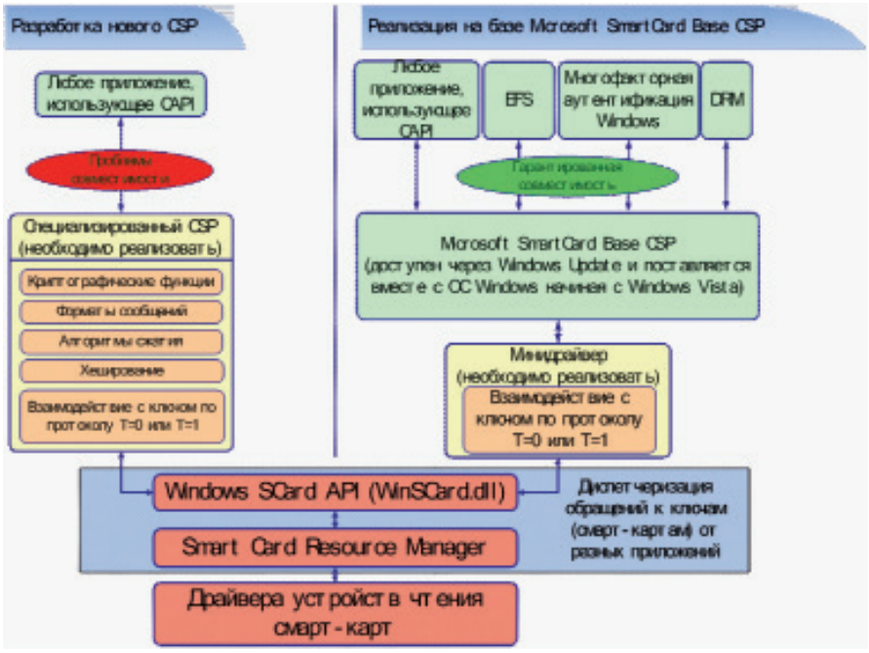


Рис. 1. Интеграция с операционной системой

Aladdin, «Актив» и другими производителями.

Новая инфраструктура поддержки смарт-карт, появившаяся в составе пакета Microsoft Smart Card Base CSP для ОС Microsoft Windows XP и Microsoft Windows Server 2003, а также реализованная в составе операционных систем Microsoft Windows Vista и Microsoft Windows Server 2008, предполагает взаимодействие системы и приложений с электронными ключами и смарт-картами без разработки специализированных крипто-сервис-провайдеров для смарт-карт. При этом функциональность, необходимая для успешной работы, обеспечивается специализированным мини-драйвером, который содержит интерфейсы, необходимые для взаимодействия со смарт-картой, но свободен от реализаций криптографических протоколов. Использование такого подхода позволило сократить временные затраты при разработке, существенно повысить качество реализаций и добиться гарантированной совместимости с приложениями, поддерживающими CryptoAPI. Различия между традиционной схемой, предполагающей разработку нового крипто-сервис-провайдера, и использованием мини-драйверов показаны на рис. 1.

Существенным недостатком архитектуры, предусматривающей разработку нового крипто-сервис-провайдера, являются также проблемы совместимости с различными приложениями и необходимость использования нестандартных утилит для выполнения основных операций с электронными ключами. Проблемы совместимости в данном случае вызваны тем, что сами крипто-сервис-провайдеры для смарт-карт и приложения, которые к ним обращаются, не всегда в полной мере соответствуют спецификациям и производятся различными производителями без прямого тестирования.

РЕШАЕМЫЕ ЗАДАЧИ

Предлагаемый программно-аппаратный комплекс средств двухфакторной аутентификации работает как в рамках стандартной инфраструктуры Windows, использующей сертификаты, так и на автономных компьютерах, используя электронный ключ для хранения учетных данных пользователя. Устройство совместимо со спецификацией USB CCID-Compliant Smart Card Reader поддерживает энергосбережение, шифрование, хеширование и цифровую подпись на ключе. Для интеграции в инфраструктуру поддержки смарт-карт в операционных системах Microsoft Windows был разработан модуль поддержки типа смарт-карт (Smart Card Minidriver). Электронный ключ имеет файловую систему с поддержкой каталогов, позволяющую операционной системе хранить файлы сертификатов. Логическая схема ключа приведена на рис. 2.

Аппаратная составляющая комплекса выполнена в виде USB-брелока, функциональность микропрограммы обеспечивает хранение цифровых сертификатов X509 на ключе, проверку PIN-кода и выполнение операций кодирования.

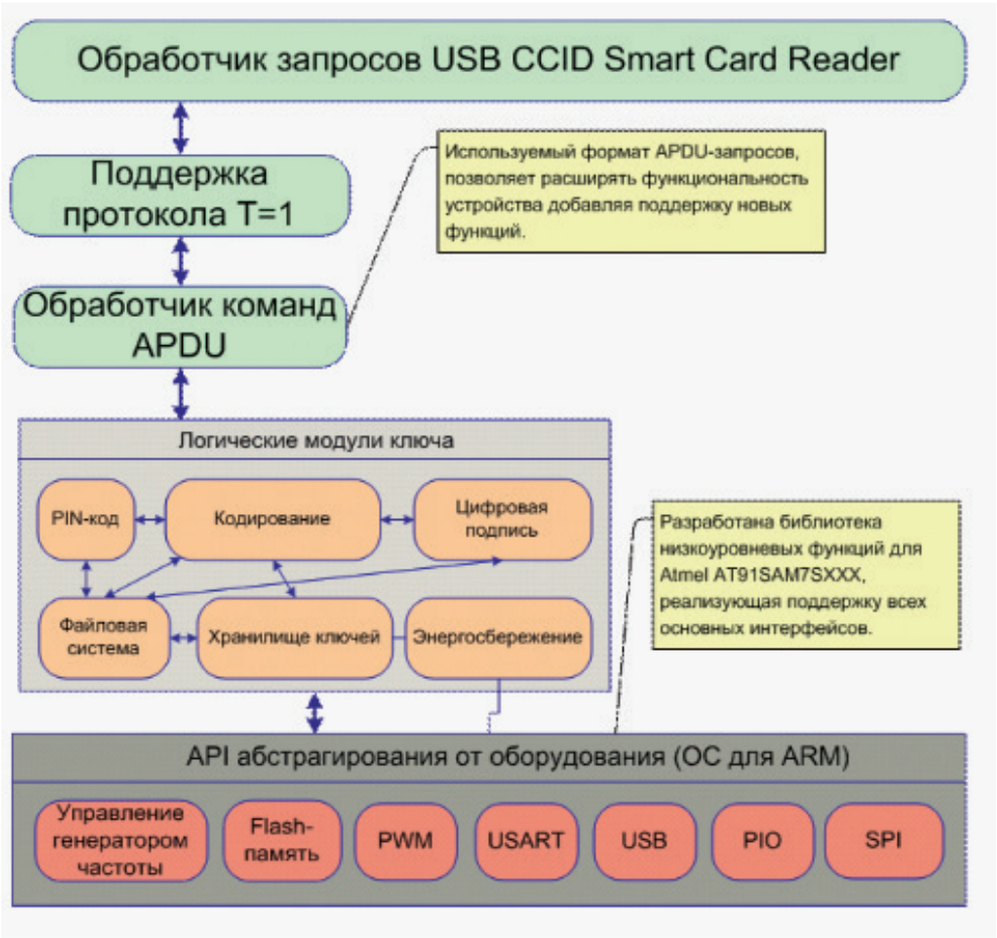


Рис. 2. Логическая архитектура USB-ключа

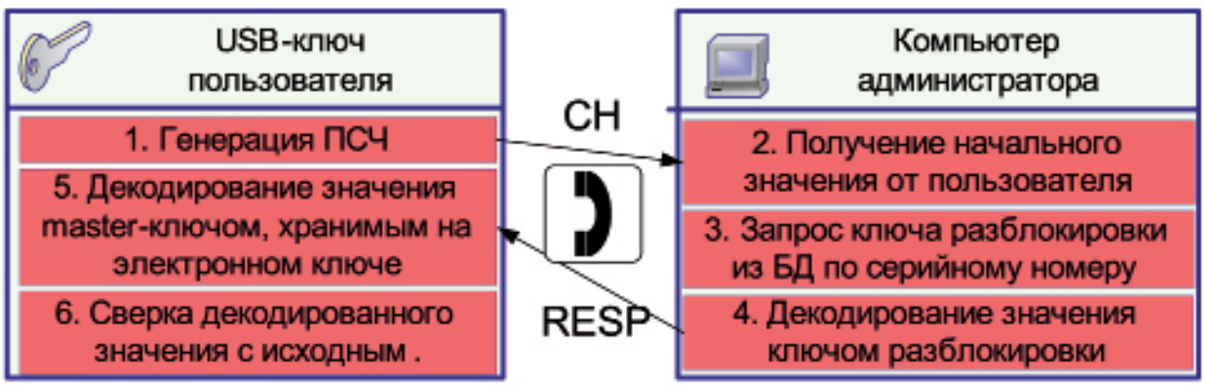


Рис. 3. Схема процесса разблокировки ключа по телефону

ДОПОЛНИТЕЛЬНАЯ ФУНКЦИОНАЛЬНОСТЬ

Отдельно следует отметить функцию защищенной аутентификации пользователей при входе в систему на автономных компьютерах, где использование стандартной Kerberos-инфраструктуры невозможно вследствие отсутствия центра сертификации. В составе решения разработаны расширения системы аутентификации для поддержки аутентификации при входе в систему с использованием сохраненных на ключе учетных данных (в том числе – разработан Credential Provider для Windows Vista и Windows Server 2008). При использовании данной функции также сохраняется возможность хранения сертификатов на ключе для использования при аутентификации на Web-сайте или в иных приложениях.

Необходимо отметить, что в случае 10 неудачных попыток ввода PIN-кода ключ переходит в заблокированное состояние. В этом случае для разблокировки ключа необходимо произвести специализированную процедуру аутентификации по протоколу (Challenge-Responce), которая предусматривает генерацию псевдослучайного значения на электронном ключе, вычисление соответствующего ему кода ответа третьей стороной и проверку правильности данного значения. Схема процесса разблокировки ключа приведена на рис. 3.

Параметры аппаратного решения позволяют хранить до 100 сертификатов в зависимости от используемой длины ключа, что превосходит характеристики большинства известных аналогов. Функционально разработанное решение имеет все необходимые для работы программные и аппаратные компоненты и может использоваться для поддержки Kerberos-аутентификации для защищенного входа пользователей в домен, аутентификации на Web-сайтах, подписи электронной почты, защиты документов Microsoft Office, а также в иных приложениях, поддерживающих инфраструктуру смарт-карт. Разработанные средства проверены, отлажены, имеют завершенный вид и ориентированы на массовое производство.

Литература

1. *Ухлинов Л.М.* Обеспечение безопасности информации в центрах обеспечения управления полетами космических аппаратов. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2000.
2. *Касперский Е.* Основные классы угроз, их причины и способы устранения. – М.: «Джет Инфо Паблишер», 2004.
3. *Соломон Д.* Внутреннее устройство Microsoft Windows 2000. – СПб.: «Питер», 2001.
4. *Ховард М.* Защищенный код. – М.: ИД «Русская редакция», 2004.
5. *Schneier B.* Applied cryptography: protocols, algorithms and source code. – NY: «Wiley», 1996.
6. *Artro S.* Public-Key cryptography. – NY: «Springer-Verlag», 1990.

Чтобы помнили...

Актер **Богдан Ступка**
27 августа 1941 — 22 июля 2012

Физик **Сергей Капица**
14 февраля 1928 — 14 августа 2012

Писатель **Гарри Гаррисон**
12 марта 1925 — 15 августа 2012

Режиссер **Тони Скотт**
21 июня 1944 — 19 августа 2012

Астронавт **Нил Армстронг**
5 августа 1930 — 25 августа 2012

Актер **Игорь Кваша**
4 февраля 1933 — 30 августа 2012

Генерал **Павел Грачев**
1 января 1948 — 23 сентября 2012

Писатель **Борис Стругацкий**
15 апреля 1933 — 19 ноября 2012

Мультипликатор **Федор Хитрук**
1 мая 1917 — 3 декабря 2012

Певица **Галина Вишневская**
25 октября 1926 — 11 декабря 2012

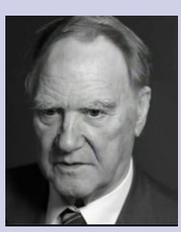
Актер **Александр Пороховщиков**
31 января 1939 — 15 апреля 2012

Стилист **Видал Сассун**
17 января 1928 — 9 мая 2012

Певец **Эдуард Хиль**
4 сентября 1934 — 4 июня 2012

Писатель **Рэй Брэдбери**
22 августа 1920 — 5 июня 2012

Режиссер **Петр Фоменко**
13 июля 1932 — 9 августа 2012



Серге́й Петро́вич Капи́ца (14 февраля 1928, Кембридж — 14 августа 2012, Москва) — советский и российский учёный-физик, телеведущий, главный редактор журнала «В мире науки». С 1973 года бессменно вёл научно-популярную телепрограмму «Очевидное — невероятное». Сын лауреата Нобелевской премии Петра Леонидовича Капицы. Принадлежит к династии русских учёных. Сын лауреата Нобелевской премии П. Л. Капицы, внук А. Н. Крылова, русского математика и кораблестроителя, и внучатый племянник известного французского биохимика Виктора Анри (Victor Henri, Крылова — по линии матери, Анны Алексеевны), правнук известного географа И. И. Стебницкого, старший брат А. П. Капицы.