# Средства многофакторной аутентификации в современной инфраструктуре безопасности информационных систем

## The means of multifactor authentication in the modern security infrastructure of information systems

**КАРМАНОВ / KARMANOV A.**
**Андрей Геннадиевич**
кандидат технических наук, доцент,
начальник Центра ситуационного анализа
ЗАО «Институт телекоммуникаций»,
Санкт-Петербург

**ГАЛИМОВ / GALIMOV T.**
**Тимур Артурович**
генеральный директор
ООО «Персонал энд Бизнес Секьюрити»,
Санкт-Петербург

**Ключевые слова:** средства многофакторной аутентификации – the means of multifactor authentication; смарт-карта – smart card; двухфакторная аутентификация– two-factor authentication.

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. 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 могут быть необоснованно дорогими. Описывается современный программно-аппаратный комплекс средств многофакторной аутентификации для систем Windows 7 /WindowsServer 2008/ Windows Vista на базе электронных ключей для шины USB, рассчитанный на применение как в государственных, так и в коммерческих организациях.

The means of multifactor authentication is an obligatory component in the security infrastructure of the modern information systems. The demanding requirements to information protection against unauthorized access bring about the necessity of developing reliable and inexpensive means of multifactor authentication of users. The majority of existing solutions on the market have various limitations: problems of compatibility and convenience of employment, outdated and complex architecture for implementation; and in many case it can be unreasonably expensive. Described below is the modern hardware and software system of the means of multifactor authentication for the system Windows 7 /WindowsServer 2008/ Windows Vista based on electronic keys for bus USB which is designed for employment in both state and commercial organizations.

### ВВЕДЕНИЕ

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 также 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 проце-

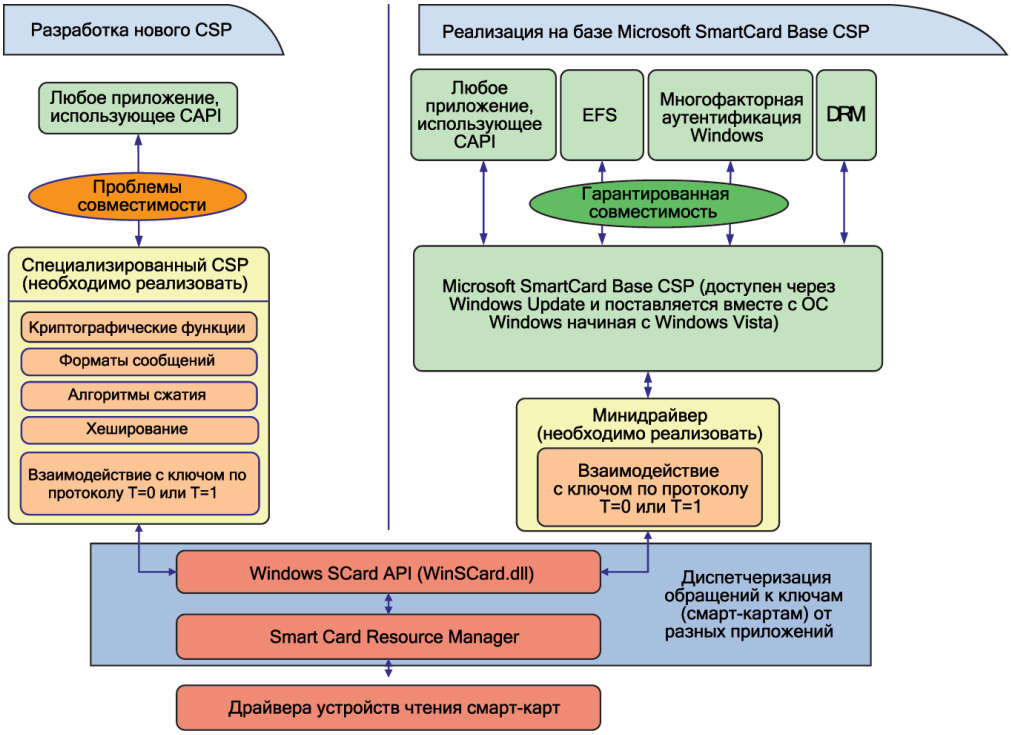


**Рис. 1.** Интеграция с операционной системой

дура 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 могут быть необоснованно дороги. Предлагается современный программно-аппаратный комплекс средств многофакторной аутентификации для систем Windows 7/ Windows Server 2008/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 криптосервис-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 от компаний Aladdin, «Актив» и других производителей.

Новая инфраструктура поддержки смарт-карт, появившаяся в составе пакета Microsoft Smart Card Base CSP для ОС Microsoft Windows 7 и Microsoft Windows Server 2008, а также реализованная в составе операционных систем Microsoft Windows Vista / 7 и Microsoft Windows Server 2008 предполагает взаимодействие системы и приложений с электронными ключами и смарт-картами без разработки специализированных криптосервис-провайдеров для смарт-карт. При этом функциональность, необходимая для работы, обеспечивается специализированным мини-драйвером,

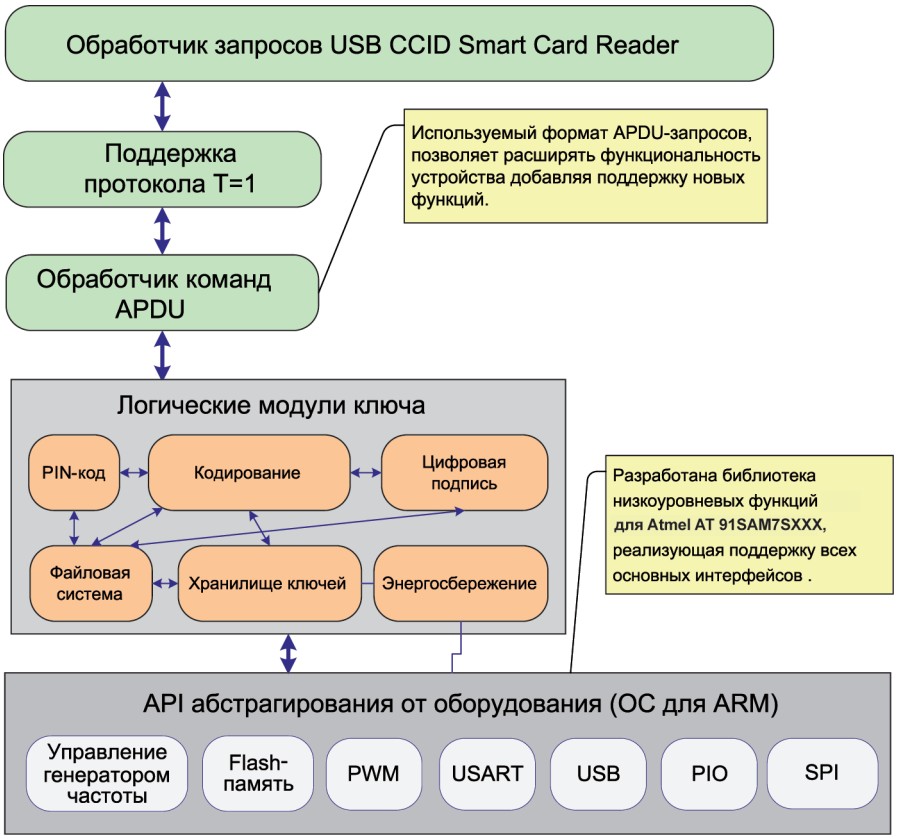


**Рис. 2.** Логическая архитектура USB-ключа

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 криптосервис-провайдера, и использованием минидрайверов показаны на рис. 1.

Существенным недостатком архитектуры, предусматривающей разработку нового криптосервис-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 криптосервис-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-CompliantSmartCardReader, поддерживает энергосбережение, шифрование, хеширование, цифровую подпись на ключе. Для интеграции в инфраструктуру поддержки смарт-карт в операционных системах Microsoft Windows был разработан модуль поддержки типа смарт-карт (SmartCardMinidriver). 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, выполнение операций кодирования.

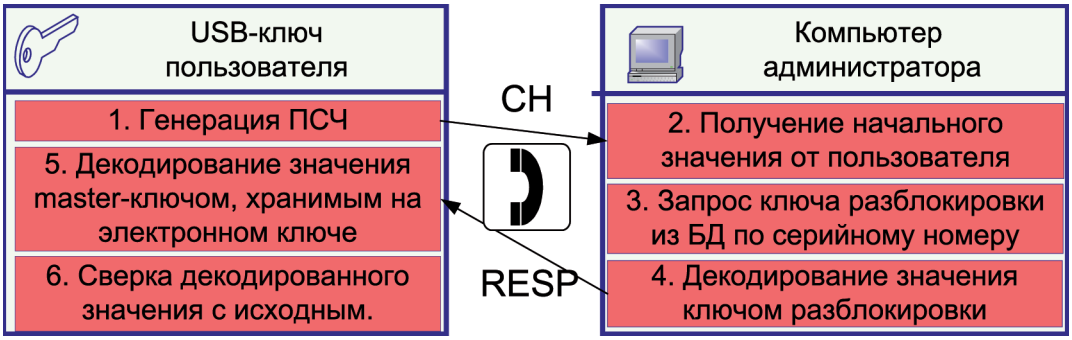


**Рис. 3.** Схема процесса разблокировки ключа по телефону

## 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 CredentialProvider для Windows 7 и Windows Server 2008). При использовании этой 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 показана на рис. 3.

## ЗАКЛЮЧЕНИЕ

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 в компьютерном сообществе 2003 г., 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 in C. – N-Y., 1996.
6. *Salomaa A.* Public-Key Cryptography. – N-Y., 1990.
7. *Russel C., Gerend J.* Microsoft Windows Server 2003 Administrator's companion. – Redmond, 2003.
8. Microsoft Corporation. MCSE Training Kit: Designing Microsoft Windows 2000 Network Security. – Redmond, 2000.