УДК 004.056.5

Я.В. Ковтун

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

АНАЛИЗ ВОЗМОЖНОСТЕЙ ИНТЕГРАЦИИ НАЦИОНАЛЬНЫХ СТАНДАРТОВ КРИПТОГРАФИИ В ОС WINDOWS

Проанализированы криптографические средства ОС Windows. Проанализированы особенности национальных криптографических стандартов.

Ключевые слова: *ДСТУ, Windows, CNG, CryptoAPI, CSP, KSP, цифровой сертификат.*

Введение

Криптография сегодня – это неотъемлемая составляющая современных информационных систем: от электронной почты и «паутины» сети Интернет до систем сотовой связи и систем электронных платежей. Криптографические методы защиты позволяют обеспечить свойства целостности и конфиденциальности данных, а также установить авторство документа и обеспечить контроль «причастности» (или неотказуемость) от факта создания электронного документа. Применение криптографии позволяет предотвратить попытки мошенничества в электронной коммерции и придать юридическую силу любому электронному документу. Криптография как позволяет однозначно установить вашу личность, так и обеспечить анонимность.

В Украине используются национальные стандарты криптографической защиты информации. Так, юридическую силу в Украине могут иметь лишь те документы, которые подписаны в соответствии с украинским стандартом электронной цифровой подписи ДСТУ 4145-2002. Естественно, для использования национальных украинских криптографических стандартов требуется соответствующее программное обеспечение.

Самым очевидным и простым подходом к реализации такого ПО является написание отдельного программного приложения, реализующего криптографические алгоритмы и необходимую бизнес-логику. Однако серьѐзным недостатком такого подхода является то, что сегодня криптография имеет множество применений. Цифровая подпись и шифрование электронных документов или почты, выдача и обслуживание цифровых сертификатов, различные защищенные соединения (к примеру, при помощи протокола HTTPS) и многое другое – реализация всех этим механизмов ложится на плечи разработчика такого ПО.

Однако наиболее распространѐнная в нашей стране ОС Windows уже реализует поддержку всех необходимых механизмов криптозащиты и стороннее программное обеспечение может использовать эти механизмы для решения прикладных задач. Единственная проблема – ОС Windows не предоставляет реализацию украинских алгоритмов. Рассмотрению вопросов, связанных с проблемой добавления поддержки национальных алгоритмов в ОС Windows, и посвящена данная статья.

Криптография в ОС Windows

В состав операционных систем Microsoft входит CryptoAPI [1] – прикладной интерфейс программирования приложений, который обеспечивает разработчиков Windows-приложений стандартным набором функций для работы с криптографической подсистемой. CryptoAPI поддерживает работу как с асимметричными так и симметричными криптоалгоритмами, то есть позволяет осуществлять весь спектр криптопреобразований. Набор алгоритмов, поддерживаемых CryptoAPI, зависит от набора криптопровайдеров (Cryptographic Service Provider, CSP), установленных в системе. CSP представляет собой динамически подключаемую библиотеку (DLL), которая реализует заданный CryptoAPI набор функций. По умолчанию с ОС Windows поставляется набор криптопровайдеров Microsoft, а также возможно добавление криптопровайдеров сторонних разработчиков. Архитектура CryptoAPI приведена на рис. 1 [1].

К сожалению, архитектура CryptoAPI имеет целый ряд серьезных недостатков. В частности, возможности по реализации криптопровайдера с нестандартными алгоритмами (то есть, отличающимися от тех, что реализованы в криптопровайдерах Microsoft) очень ограничены из-за ограничений архитектуры.

Поэтому, начиная с Windows Vista, на смену CryptoAPI пришел Cryptography API: Next Generation (CNG). CNG имеет более гибкую, по сравнению с CryptoAPI, архитектуру. CNG поддерживает все алгоритмы, поддерживаемые CryptoAPI, а также некоторые другие, в частности, алгоритмы, основанные на эллиптических кривых над конечными полями. CNG поддерживает криптопровайдеры, работающие как на пользовательском режиме, так и в режиме ядра.

Одним из главных отличий CNG от CryptoAPI является разделение провайдеров, реализующих криптографические примитивы (шифрование, хеширование и пр.), и провайдеров, отвечающих за надежное хранение секретных ключей. Последние

получили название Key Storage Providers (KSP). Архитектура криптографических примитивов CNG приведена на рис. 2. Архитектура хранения ключей CNG приведена на рис. 3 [1].

Рассмотрим преимущества CNG над CryptoAPI применительно к реализации нового типа криптопровайдера.

Как было сказано выше, CNG четко отделяет хранение ключей от криптографических преобразований. В CryptoAPI обе эти функции «ложились на плечи» одного провайдера.

Еще одно важно отличие – разделение понятий «провайдер» и «асимметричный алгоритм». В CryptoAPI каждый провайдер мог реализовать лишь один алгоритм цифровой подписи и один алгоритм формирования общего секрета либо асимметричного шифрования. Как видно из рис.2, в CNG введены понятия алгоритма цифровой подписи, алгоритма асимметричного шифрования и алгоритма формирования общего секрета. Это значит, что один криптопровайдер может реализовать любое количество асимметричных алгоритмов.

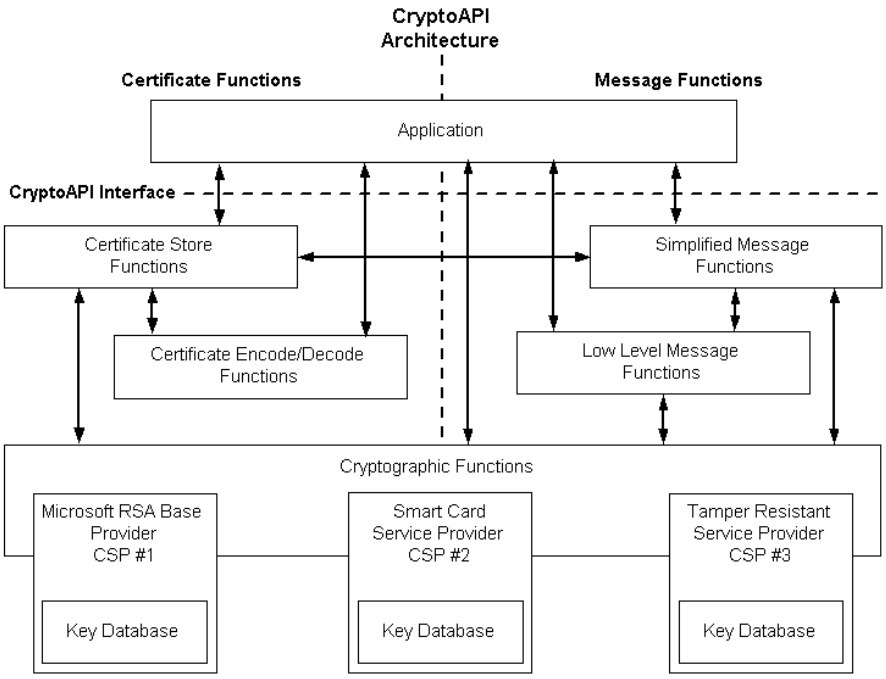

Рис. 1. Архитектура CryptoAPI

Но, пожалуй, главное преимущество CNG при реализации нового типа криптопровайдера далеко не очевидно. Дело в том, что продукты Microsoft, использующие CryptoAPI, написаны в основном с расчетом лишь на использование криптопровайдеров Microsoft. Например, при установке Active Directory Certificate Services неизвестные типы провайдеров просто игнорируются. Или же, при подсчете хэша сертификата разработчики компании Microsoft предполагают, что максимальная длина хэша – 20 байт и резервируют статический буфер размером 20 байт, вместо того, чтобы сделать вызов функции, определяющий размер хэша. Это справедливо при использовании провайдеров Microsoft, реализующих алгоритмы MD-5 или SHA-1 (у которых размер хэш-дайджеста не превышает 160 бит). Однако такой подход приводит к проблемам при реализации, например, алгоритма ГОСТ 34.311-95 [2], размер хэш-дайджеста которого 32 байта. Нередко используются недокументированные функции, которые также работают только с криптопровайдерами Microsoft. Поэтому при реализации криптопровайдеров для CryptoAPI приходилось использовать массу «обходных» приемов, которые, как правило, сводились к модификации кода библиотек Microsoft, что противоречит изначальной идее использования криптопровайдера, как средства расширения поддерживаемых средств криптозащиты в рамках единой идеологии построения системы безопасности. К счастью, при реализации CNG, разработчики Microsoft учли недостатки предыдущей архитектуры и подобных проблем не возникает (или, по крайней мере, их стало гораздо меньше).

Особенности украинских стандартов

На Украине рекомендованы к применению 4 стандарта: один стандарт (симметричного шифрования) бывшего СССР – ДСТУ ГОСТ 28147:2009; два межгосударственных (Азербайджан, Беларусь, Казахстан, Киргизия, Таджикистан, Россия, Туркменистан, Украина) стандарта (ГОСТ 34.310-95 – цифро-

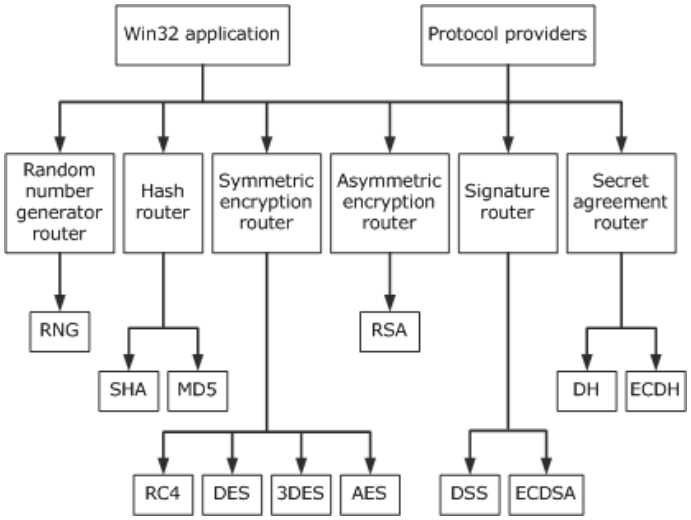

Рис. 2. Архитектура криптографических примитивов CNG

вая подпись, ГОСТ 34.311-95 – хэш-функция), и один стандарт Украины (ДСТУ 4145-2002 – цифровая подпись).

Стандарты, принятые в Украине для электронной цифровой подписи (ЭЦП), тоже имеют свою особенность. Как известно, для формирования цифровой подписи создается пара ключей — открытый ключ, предназначенный для проверки подписи, и секретный (личный), предназначенный для наложения (создания) подписи. Проблема в том, что алгоритмы цифровой подписи, которые приняты в Украине, имеют еще один ключевой элемент – так называемый Долгосрочный ключевой элемент (ДКЭ), который представляет собой заполнение узлов замены таблицы подстановок хеш-функции ГОСТ 34.311-95 и, фактически, является параметром алгоритма ЭЦП , т.к. он используется при формировании и проверке ЭЦП [3, 4].

Фактически ДКЭ – это таблица подстановок (S-Box), использующаяся в алгоритме шифрования ДСТУ ГОСТ 28147:2009, на котором основан хэш-алгоритм ГОСТ 34.311-95. Это значит, что при подсчете хэш-функции для формирования цифровой подписи в качестве дополнительного параметра должен быть передан ДКЭ. Конечно же, в Microsoft не заложена поддержка подобного механизма, а, значит, при реализации криптопровайдера с поддержкой украинского стандарта ЭЦП необходимо решить задачу установки дополнительного параметра алгоритма ЭЦП.

Одним из ключевых элементов инфраструктуры открытых ключей (PKI) является сертификат открытого ключа – цифровой документ, подтверждающий принадлежность указанного открытого ключа, идентифицированному в сертификате субъекту (владельцу). В Украине принят стандарт формата таких сертификатов, основанный на стандарте X.509 [5]. Однако у нашего стандарта есть ряд особенностей, затрудняющих реализацию его поддержки. Сертификат в формате X.509 представляет собой структуру объектов, закодированную согласно ASN.1. У каждого объекта в этой структуре есть свой идентификатор (OID). В структуре сертификата присутствуют такие объекты, как алгоритм открытого ключа (представляет собой асимметричный алгоритм цифровой подписи) и алгоритм цифровой подписи (представляет собой асимметричный алгоритм цифровой подписи плюс хэш-алгоритм). Особенностью украинского стандарта является то, что для обоих этих понятий используется один и тот же OID (в случае ДСТУ 4145-2002 в полиномиальном базисе – 1.2.804.2.1.1.1.1.3.1.1).

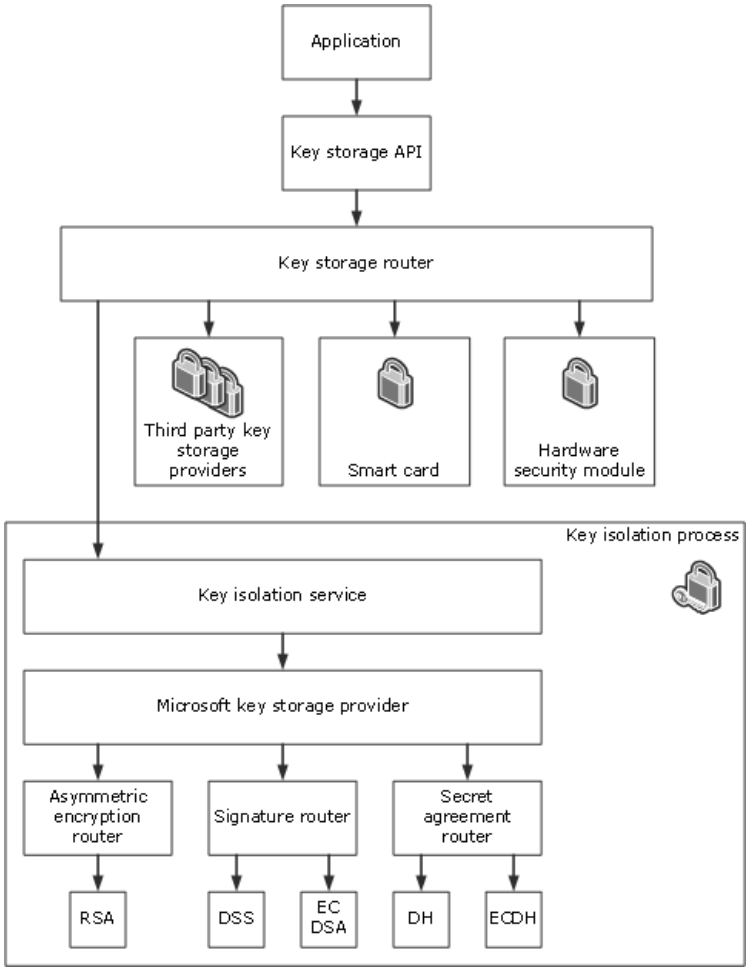

Рис. 3. Архитектура хранения ключей CNG

Реализация криптопровайдера CNG

Рассмотрим шаги, необходимые для реализации криптопровайдера CNG с учетом ранее упомянутых особенностей национальных стандартов в области криптографии.

Первым и наиболее очевидным шагом является собственно реализация набора алгоритмов цифровой подписи, хеширования и симметричного шифрования, а именно: ДСТУ 4145, ГОСТ 34.311, ГОСТ 28147. Для этого необходимо реализовать набор функций провайдера алгоритмов и провайдера хранения ключей. Прототипы и назначение данных функций подробно описаны в документации, поставляемой с Microsoft CNG Development Kit [6]. Регистрация реализованного провайдера в системе производится при помощи вызова функции BCryptRegisterProvider.

Первый шаг, описанный выше, является необходимым для реализации любого криптопровайдера CNG. Рассмотрим, какие дополнительные шаги необходимо проделать, учитывая особенности национальных стандартов.

Поскольку ОС Windows по умолчанию не имеет поддержки национальных криптоалгоритмов, соответствующие объектные идентификаторы (OID)

также изначально не зарегистрированы. Для регистрации OID используется функция CryptRegisterOIDInfo [1]. Список объектных идентификаторов, использующихся в национальном стандарте, приведен в [5]. Регистрация данных объектных идентификаторов позволяет сопоставить алгоритмы, реализуемые криптопровайдером, с алгоритмами, применяемыми в сертификатах открытых ключей и прочих объектах. Особое внимание стоит уделить ранее упомянутому идентификатору 1.2.804.2.1.1.1.1.3.1.1 – его следует зарегистрировать и в качестве алгоритма открытого ключа (CRYPT_PUBKEY_ALG_OID_GROUP_ID), и в качестве алгоритма цифровой подписи (CRYPT_SIGN_ALG_OID_GROUP_ID).

Для поддержки национального формата сертификатов открытых ключей также необходимо реализовать и зарегистрировать OID-функции: CRYPT_OID_VERIFY_ENCODED_SIGNATURE_FUNC, CRYPT_OID_IMPORT_PUBLIC_KEY_INFO_EX2_FUNC, CRYPT_OID_EXPORT_PUBLIC_KEY_INFO_EX2_FUNC, CRYPT_OID_SIGN_AND_ENCODE_HASH_FUNC.

Регистрация производится при помощи функции CryptRegisterOIDFunction [1]. Реализация этих функций необходима, поскольку открытые ключи и цифровые подписи, хранящиеся в сертификатах, имеют особый формат, описанный в [5].

Наконец, для корректной проверки цифровой подписи сертификатов открытого ключа необходимо учитывать упомянутый ранее ДКЭ. Поскольку архитектура CNG не предусматривает использование механизма ДКЭ, требуется соответствующим образом изменить работу функции Win32 API CertGetCertificateContextProperty с параметром CERT_SIGNATURE_HASH_PROP_ID [1], производящей расчет хеша сертификата. Описание способов подобной модификации функций Win32 API выходит за рамки данной статьи.

Заключение

Существует несколько способов реализации программного обеспечения, использующего криптографию. Одним из способов является добавление в ОС Windows требующихся криптоалгоритмов путѐм написания специального модуля – криптопровайдера. Существует два вида криптопровайдеров – CSP для CryptoAPI и для CNG. CNG является более новой технологией, появившейся в Windows Vista и имеющей ряд существенных преимуществ. Поэтому при реализации новых криптопровайдеров рекомендуется использовать именно CNG.

Национальные стандарты в области криптографии имеют ряд особенностей и недостатков, затрудняющих реализацию соответствующих алгоритмов. Реализация криптопровайдера для Windows с поддержкой национальных стандартов возможна, хотя разработчику такого провайдера придется столкнуться с рядом нетривиальных проблем.

Список литературы

1. *Security // MSDN Library [Электронный ресурс]. – Режим доступа к ресурсу: http://msdn.microsoft.com/en-us /library/ee663293.aspx.*
2. *ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хэширования. Введ. 16.04.1998. – К.: Госстандарт Украины, 1998. – 16 с.*
3. *Белов С., Мартыненко С. Юстас – Алексу [Электронный ресурс]. – Режим доступа к ресурсу: http://kontrakty.com.ua/ show/rus/article/2/0620066871.html.*
4. *Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації, що реалізують криптографічний алгоритм, визначений ГОСТ 28147-89 від 12.06.2007р. [Электронный ресурс]. – Режим доступа к ресурсу: http://zakon.rada. gov.ua/cgi-bin/laws/main.cgi?nreg=z0729-07.*
5. *Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, Державного департаменту з питань зв'язку та інформатизації Міністерства транспорту та зв'язку України №99/166. Національна система електронного цифрового підпису. Технічні специфікації форматів представлення базових об'єктів [Электронный ресурс]. – Режим доступа к ресурсу: http://www.stc.gov.ua/ document/68848/DOC1474.PDF.*
6. *Microsoft® Windows® Cryptographic Next Generation Software Development Kit [Электронный ресурс] – Режим доступа к ресурсу: http://www.microsoft. com/downloads/ en/details.aspx?FamilyID=1ef399e9-b018-49db-a98b-0ced7cb8ff6f.*

Поступила в редколлегию 6.09.2010

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

АНАЛІЗ МОЖЛИВОСТЕЙ ІНТЕГРАЦІЇ НАЦІОНАЛЬНИХ СТАНДАРТІВ КРИПТОГРАФІЇ В ОС WINDOWS

Я.В. Ковтун

Проаналізовано криптографічні засоби ОС Windows. Проаналізовано особливості національних криптографічних стандартів.

Ключові слова: *ДСТУ, Windows, CNG, CryptoAPI, CSP, KSP, цифровий сертифікат.*

THE ANALYSIS OF NATIONAL CRYPTOGRAPHIC STANDARDS INTEGRATION INTO WINDOWS OS

Y.V. Kovtun

Windows cryptographic technologies are analyzed. Features of national cryptographic standards are analyzed.

Keywords: *DSTU, Windows, CNG, CryptoAPI, CSP, KSP, digital certificate.*