УДК 355.405.2

АНАЛИЗ СТРУКТУРЫ ЦИФРОВОЙ ПОДПИСИ ФОРМАТА PKCS#7

Макар А. А.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: канд. техн. наук Ролич О. Ч.

Аннотация. Статья посвящена цифровой подписи в формате PKCS#7. В ней проанализированы возможности единственного криптопровайдера Avest CSP в Республике Беларусь. Проанализированы возможности использования CryptoAPI.

Ключевые слова: криптопровайдер, АВЕСТ, AvCSP, Microsoft CryptoAPI, PKCS#7

Введение. Актуальность темы связана с ежедневным использованием электронных документов и защиты информации. Взаимодействие с документами зарастает электронно-цифровыми аспектами: размеры информационных потоков и хранилищ, обрабатывающихся в цифровом виде, каждый день вырастают, при этом «неповоротливые», в части использования свежайших технологий организации, такие как административные, судебные, исполнительные организации, все больше массово используют цифровые документы и услуги. Учитывая нюансы, с которыми сталкиваются организации при подписании документов и перевыпуске сертификатов непросто недооценить значимость электронной подписи.

Целью данной работы является анализ работы криптографии по средствам CryptoAPI и возможностей, набора механизмов и процедур защиты активов информационных систем криптопровадйером Avest CSP.

Основная часть. На протяжении последнего времени, количество документов нуждающихся в доверенности растёт с каждым днем. Для достоверности документов используется электронная цифровая подпись – это аналог рукописной подписи. Она выполняет ту же функцию – обеспечивает юридическую значимость для документов. Кроме того, электронная подпись фиксирует информацию, которая была в документе на момент подписания, тем самым подтверждая её неизменность.

Электронная подпись состоит из двух основных частей:

1. Открытый ключ, он же сертификат.
2. Закрытый ключ – криптографическая часть.

Эти составные части выполняют разные функции: с помощью закрытого ключа, доступного только владельцу, документ шифруется, а с помощью сертификата, доступного для всех, документ дешифруется. Таким образом, достигается цель использования ЭЦП – подтверждается то, кем был подписан документ, и заверяется его неизменность с момента подписания.

PKI (Public Key Infrastructure, инфраструктура открытых ключей) – набор средств, распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей.

Аналог – это RSA ключи для SSH, но инфраструктурой их назвать сложно, так как отсутствует централизованный механизм управления ими. Также разница в том, что публичная часть ключа в паре ключей для SSH неизменна, а сертификат (публичную часть ключа участника PKI) можно перевыпустить в любой момент.

В PKI существует один или несколько Certification Authority – это центр сертификации (удостоверяющих центров) в роли который выступает НЦЭУ, отдающих публичные части своих ключей клиентам, которые в обязательном порядке перевыпускаются каждый месяц подписанные ими сертификаты. Таким образом, между участниками инфраструктуры появляются доверительные отношения, кто ими управляет, и действителен ли сертификат, выданный им или их «товарищам», в настоящий момент времени (одним из важнейших атрибутов сертификатов является срок их действия). Либо же сервер, у которого есть

публичная часть ключа СА инфраструктуры, в которой он и его клиенты работают, понимает, что к нему пришел клиент с действительным сертификатом, и разрешает ему что-то, или запрещает в противном случае.

Информация, необходимая для работы PKI, содержится в сертификате X.509. В PKI участвуют как минимум три стороны. Например, Евгений, Борис и удостоверяющий центр (УЦ) на рисунке 1. У Евгения и Бориса есть сертификаты с закрытым ключом, подписанные так называемым корневым сертификатом УЦ. У Евгения есть сертификат Бориса с открытым ключом, а у Бориса – сертификат Евгения с открытым ключом. Евгений и Борис доверяют УЦ и благодаря этому могут доверять друг другу.

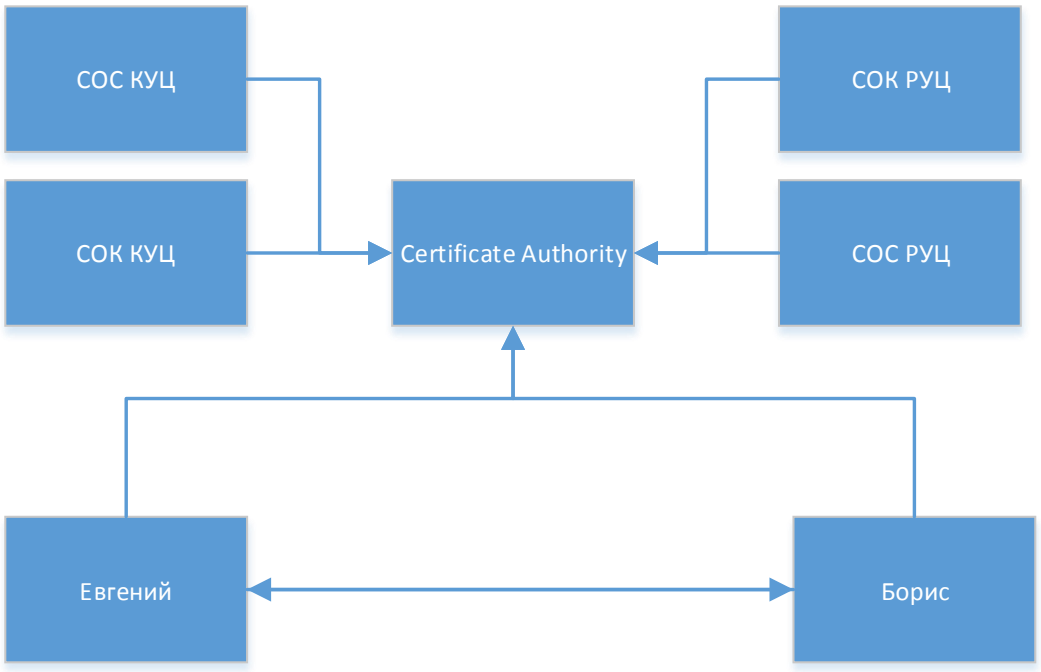

Рисунок 1 – Схематичное представление концепции работы доверенности сертификатов

Результатом прикрепленной подписи будет CMS (Cryptography Message Syntax) — сообщение, содержащее как подписываемые данные, так и саму подпись на рисунке 2. Откреплённая подпись содержит только саму подпись.

Синтаксис криптографических сообщений (CMS) используется для цифровой подписи, расшифрования или шифровать произвольное содержимое сообщения. В этой сопутствующей спецификации описывается использование общих криптографические алгоритмы с CMS. Реализации CMS может поддерживать эти алгоритмы.

Значения CMS генерируются с использованием ASN.1 [X.208-88], с использованием BER–кодирования [X.209-88]. Идентификаторы алгоритмов (включая ASN.1 идентификаторы объектов) идентифицируют криптографические алгоритмы, а некоторые алгоритмы требуют дополнительных параметров. При необходимости параметры указаны со структурой ASN.1. Идентификатор алгоритма указывается для каждого алгоритма и, при необходимости, структура параметров.

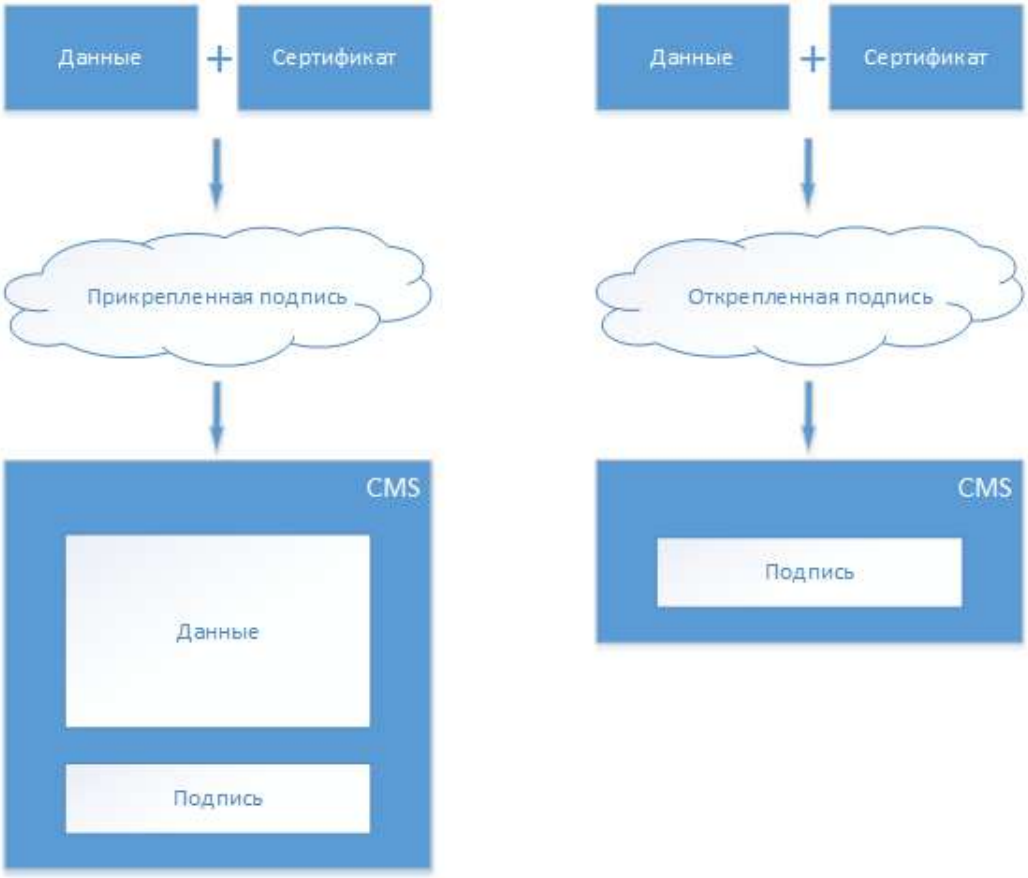

Рисунок 2 – Схематическое представление содержания CMS

Процесс подписания данных включает в себя следующие шаги:

1. Для каждой подписывающей стороны вычисляется дайджест сообщения с дайджестом сообщения для подписавшего. (Если два подписывающих лица используют один и тот же дайджест сообщения, то дайджест сообщения необходимо вычислить только один из них). Если подписывающий удостоверяет подлинность любой информации, кроме содержания, дайджест сообщения содержимого и другая информация обработанного алгоритмом дайджеста сообщения подписывающей стороны.

2. Для каждой подписывающей стороны дайджест сообщения и связанная с ним информация шифруется закрытым ключом подписавшего.

3. Для каждой подписывающей стороны дайджест зашифрованного сообщения и другая информация, относящаяся к подписанту, собирается в Значение SignerInfo. Сертификаты и списки отзыва сертификатов для каждой подписывающей стороны.

4. Алгоритм дайджеста сообщений собирает значения SignerInfo для всех подписантов вместе с содержимым в значение SignedData.

Заключение. Крупные компании занимаются разработкой API для увеличения возможностей как разработчиков относительно кода, так и пользователей, которые имеют возможность активного использования широкой функциональности большинства приложений.

Криптопровайдер AvCSP позволяет использовать вышеуказанные криптографические алгоритмы через программный интерфейс Microsoft CryptoAPI версий 1.0 и 2.0.

Такой подход имеет следующие достоинства:

1. Разработчики программных средств могут использовать криптографические функции, встроенные в операционные системы Microsoft Windows, используя для этого высокоуровневые (CryptoAPI 2.0) или низкоуровневые (CryptoAPI 1.0) функции или CAPICOM-интерфейс.

2. Становится возможным использование перечисленных криптоалгоритмов в уже разработанных или разрабатываемых независимо от криптопровайдера AvCSP продуктах, использующих Microsoft CryptoAPI.

3. Автоматически (за счёт использования CryptoAPI 2.0) обеспечивается поддержка международных форматов представления криптографических данных (сообщений, ключевой информации и т.д.). В частности, используемые форматы удовлетворяют рекомендациям X.509 и стандартам семейства PKCS (PKCS#7, PKCS#8, PKCS#10, PKCS#12).

Проведённый анализ возможностей, набора механизмов и процедур защиты активов информационных систем криптопровадйером показывает сильные стороны как для разработки новых продуктов с доступом к подписанию по средствам CryptoAPI, так и широкие возможности для использования юридических лиц и компаний.

Соответствие всех вышеуказанных алгоритмов библиотеки AvC требованиям ТНПА Республики Беларусь подтверждено сертификатами и экспертными заключениями Оперативно-аналитического центра при Президенте Республики Беларусь.

Список литературы

1. *Datatracker RFC2315 [Электронный ресурс]. – Электронные данные. Режим доступа: https://datatracker.ietf.org/doc/html/rfc2315.*
2. *Datatracker RFC3370 [Электронный ресурс]. – Электронные данные. Режим доступа: https://datatracker.ietf.org/doc/html/rfc3370.*
3. *NCEU [Электронный ресурс]. – Электронные данные. Режим доступа: https://nces.by/pki/info/software.*
4. *AvestCSP[Электронный ресурс]. – Электронные данные. Режим доступа: http://ca.ncmps.by/userfiles/file/AvCSP.pdf.*

UDC 355.405.2

ANALYSIS OF THE STRUCTURE OF THE DIGITAL SIGNATURE OF THE PKCS#7 FORMAT

Makar A. A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Rolich O.Ch. – PhD, assistant professor, associate professor of the department of ICSD

Annotation. The article is devoted to the digital signature in PKCS#7 format. It analyzes the capabilities of the only crypto provider Avest CSP in the Republic of Belarus. The possibilities of using CryptoAPI are analyzed.

Keywords. cryptoprovider, AVEST, AvCSP, Microsoft CryptoAPI, PKCS#7