УДК 681.3:002.651.028(083.73)

А.О. Мелащенко

НАЦИОНАЛЬНАЯ ЛОКАЛИЗАЦИЯ УСЛУГ ЭЛЕКТРОННЫХ ЦИФРОВЫХ ПОДПИСЕЙ В СОВРЕМЕННЫХ ОФИСНЫХ ПАКЕТАХ

Описан типовой процесс подписания, исходя из требований эталонной модели квалифицированной инфраструктуры открытых ключей. Проведено сравнение технологических возможностей офисного пакета MS Office 2010 и типового процесса подписания. Даны конкретные рекомендации по национально-украинской локализации офисного пакета MS Office 2010.

Введение

Достижение интероперабельности национальной системы электронных цифровых подписей (НСЭЦП) не обходимо, но не достаточно для внедрения информационных технологий (ИТ), основанных на ЭЦП. Достаточным условием развёртывания – поддержка эталонной модели квалифицированной инфраструктуры открытых ключей (QPKI) [1] в современных офисных пакетах как инструментах электронных бизнесов.

Цель работы – исследовать уровень поддержки QPKI в современных офисных пакетах, в первую очередь MS Office как наиболее распространённом, а также предложить конкретные шаги для национально-украинской локализации услуг ЭЦП в MS Office 2010.

1. Общий бизнес-сценарий создания электронного документа

Перед исследованием шагов для локализации формализуем процесс подписывания и определим необходимые компоненты для создания электронного документа (ЭД).

Эталонный процесс создания ЭД согласно QPKI показан на рис. 1, где:

1) документ – электронный документ любого стандартного формата, например, OpenXML[2], ODF[3], ebXML msg[4];

2) сертификат открытого ключа – X.509-сертификат, содержащи открытый ключ, параметры криптоалгоритма и необходимые данные для ассоциации с человеком [5];

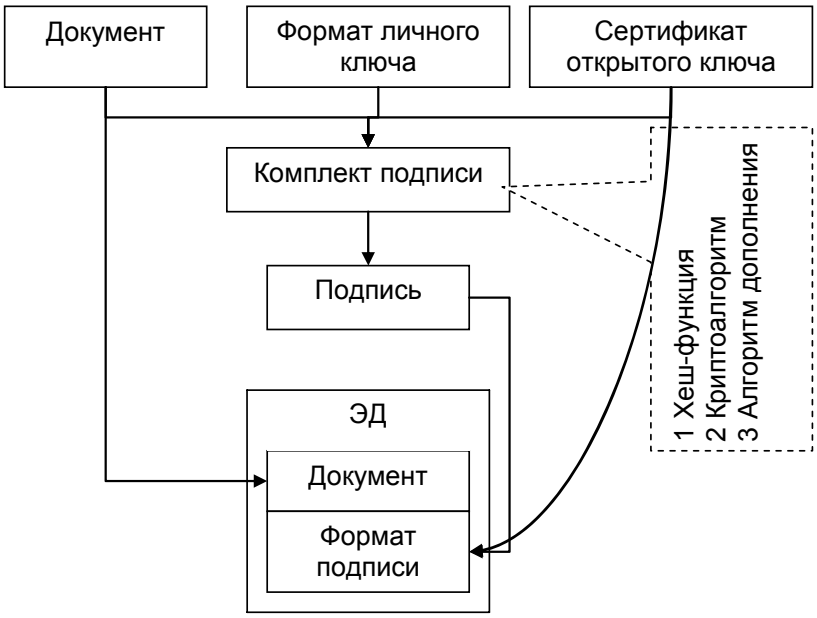

Рис. 1. Эталонный процесс создания ЭД

3) формат личного ключа – отсутствует в эталонной модели QPKI, поскольку личный ключ генерирует и физически защищает безопасное средство создания подписей (SSCD). Все операции генерации и подписания происходят внутри SSCD, ввиду чего не требуется стандартизация формата личного ключа. API SSCD соответствует ДСТУ EN 14890:2008 [6]. В противовес Директиве 1999/93/ЕС [7] (далее Директива) Закон Украины [8] позволяет одновременно использовать программные и программно-аппаратные средства для создания квалифицированных подписей, как следствие, для форматов личного ключа допустимо использование де-факто стандартов PKCS#8 и PKCS#12;

4) комплект подписи – хеш-функции и криптоалгоритмы, определенные в ДСТУ ETSI TS 102 176-1:2009;

5) электронный документ – согласно Закону Украины [9] обязательным атрибутом ЭД является ЭЦП. На рис. 1 подразумевается любые стандартные форматы ЭД (например, OpenXML, ODF, PDF и т. п.);

6) формат подписи – допустимые форматы определены в ДСТУ ETSI TS 101 903:2009, ДСТУ ETSI TS 101 733:2009, помимо фактического значения подписи содержат необходимую для верификации информацию разной степени детализации и реализуют бизнес-модель подписания согласно ДСТУ ETSI TR 101 045:2009.

2. Локализация услуг ЭЦП в офисном пакете MS Office

Рассмотрим локализацию услуг ЭЦП для формата ЭД в OpenXML. Схема реализация эталонного подписания в MS Office показана на рис. 2.

Для идентификации действий по локализации отразим реализацию процесса подписания согласно эталонной модели QPKI (рис. 3) и сравним ее с реализацией в MS Office.

Для оценки сроков и возможности модификации MS Office приведем пример интеграции в течении 6 месяцев в MS Windows уникального комплекта подписей ГОСТ34.311 + ДСТУ 4145, реализованного как «Библиотека функций криптографических преобразований «UPGCrypto-ProviderBasic»» [10] согласно спецификации MS CryptAPI.c

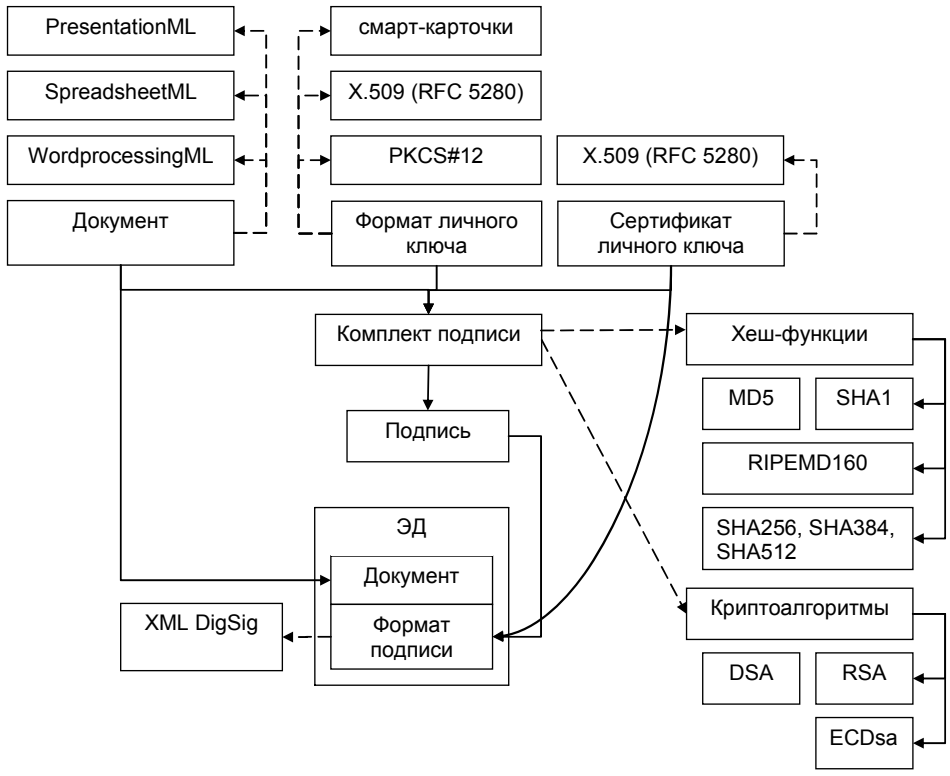

Рис. 2. Реализация эталонного процесса подписания в MS Office

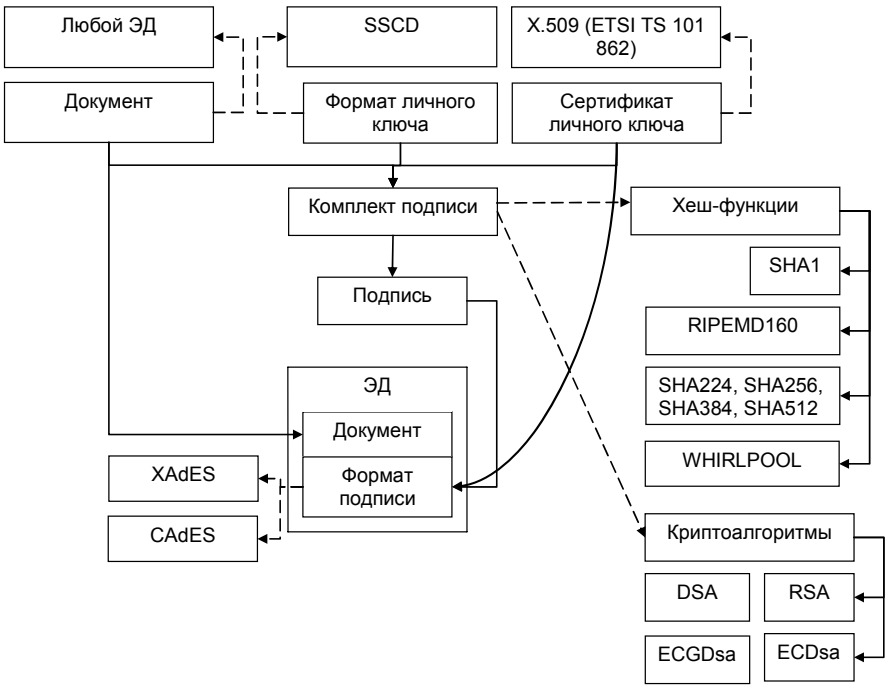

Рис. 3. Реализация эталонного процесса подписи согласно QPKI

Следовательно, для локализации услуг ЭЦП, реализованных в MS Office 2010, необходимо совершить действия отображенные на рис. 4, на котором две сущности «Документ» и «Формат личного ключа» не требуют переработки. Пунктиром с точкой выделены компоненты, которые необходимо доработать, пунктиром выделеные – компоненты, доработка которых является опциональной.

Необходимые шаги для локализации MS Office 2010.

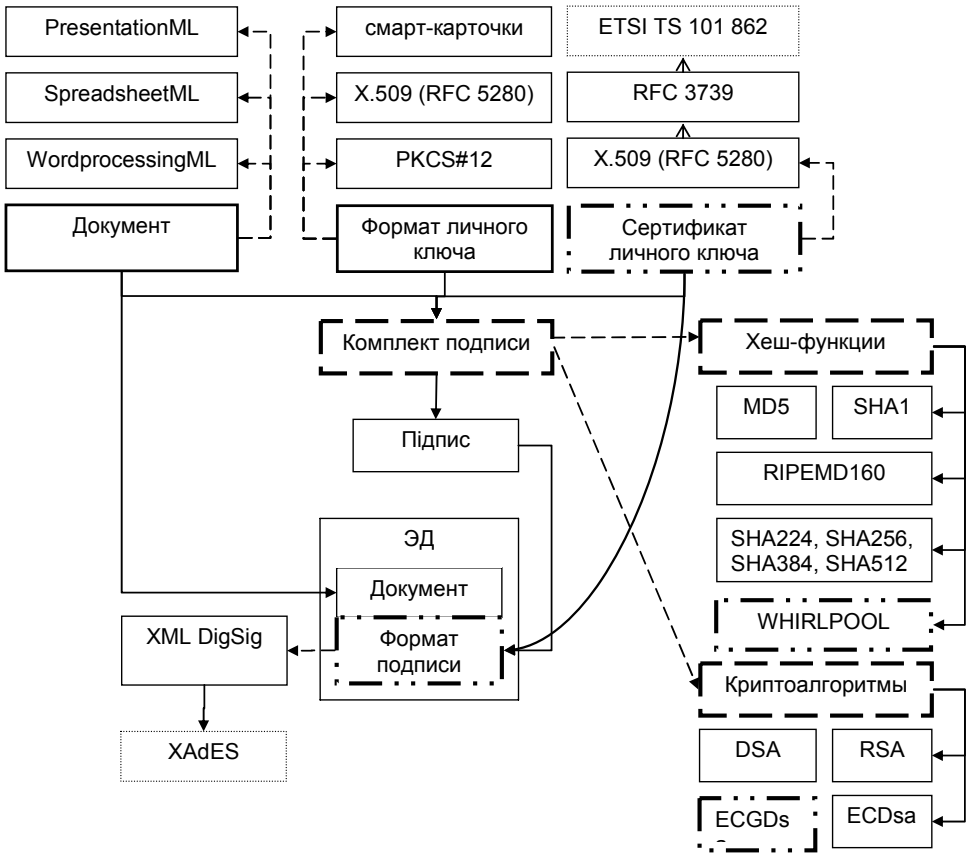

Рис. 4. Необходимые действия по доработке MS Office 2010

1. Реализовать формат сертификата открытого ключа в соответствии с ДСТУ ETSI TS 101 862:2009 (рис. 5, а). Этот стандарт основан на RFC 3739, который в свою очередь профилирует RFC 5280, реализованный в версии MS Windows 2000 и выше, необходимо сначала реализовать RFC 3739 на основе RFC 5280, а затем – ДСТУ ETSI TS 101 862:2009 на основе RFC 3739.

2. Реализовать формат подписи XAdES. Заметим, что реализация этого формата требует не изменения стандартов OpenXML, а лишь реализации расширений XMLDigSig согласно ДСТУ ETSI TS 101 903:2009 и профиля ДСТУ ETSI TS 102 904:2009 (рис. 5, б). Рекомендуется реализовать формат подписи CAdES согласно ДСТУ ETSI TS 101 733:2009 и профилю ДСТУ ETSI TS 102 734:2010 в среде MS Windows для имплементации юридических требований QPKI стандартными средствами MS Windows.

3. Согласно Директиве квалифицированные подписи обрабатываются SSCD. С позиций эталонной модели QPKI, поддерживающей Директиву, эти устройства соответствуют стандартам ДСТУ EN 14890 и CWA 14169. Необходимо установить, является ли степень поддержки семейством MS Windows широкого диапазона SSCD, тогда можно интегрировать драйверы наиболее употребимых устройств (рис. 6).

4. Необходимо исследовать реализацию в семействе операционных сред MS Windows требований безопасности для приложений создания подписей согласно ДСТУ CWA 14170:2009 и общих рекомендаций для верификации электронных подписей в соответствии с ДСТУ CWA 14171:2009 (рис. 6).

5. Необходимо исследовать соответствие реализуемой системы управления сертификатами семейства MS Windows Server стандарту CWA 14167-1 и стандартных модулей подписания частям 2,3,4 серии CWA 14167 (рис. 6).

6. Необходимо реализовать в инфраструктуре MS Windows Server сервер и клиент службы штемпелевания времени согласно требованиям ДСТУ ETSI TS 101 861:2009.

Опционально целесообразно реализовать поддержку алгоритма подписания ECGDsa и хеш-функции WHIRLPOOL. Заметим, что реализация хеш-функции WHIRLPOOL значительно улучшит безопасность MS Windows, ввиду современного алгоритма хеширования, отличного от схемы sha1 и sha2, которая пока единственная реализована среди алгоритмов хеширования в семействе MS Windows.

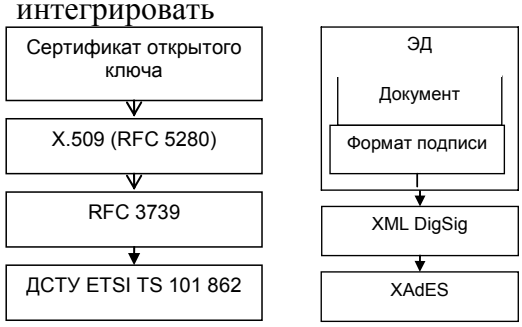

Рис. 5. Иллюстрация необходимых этапов доработки существующих реализаций

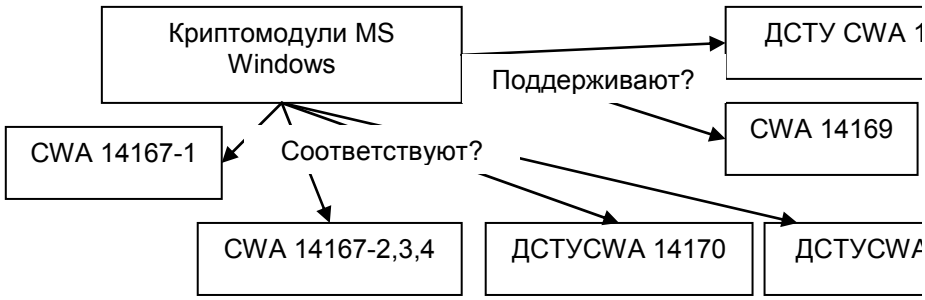

Рис. 6. Иллюстрация объектов стандартных криптомодулей семейства MS Windows.

Выводы

Учитывая разделение функциональной нагрузки на серверную часть (например, реализация PKI в MS Windows Server 2008 R2) и на клиентскую (например, MS Office 2010 + MS Windows 7), необходимо реализовать минимум функций в клиентской части и провести углубленные исследования серверной части на предмет соответствия европейским стандартам QPKI. Заметим, что доработки только расширят существующие функции и улучшат безопасность систем, использующих ЭЦП. Укажем на отсутствие потребности в пересмотре международных стандартов, в частности OpenXML для выполнения требований эталонной модели QPKI.

Реализация требований без дополнительной модификации обеспечит национальную локализацию продуктов Microsoft (в частности Windows и Office'2010) для организации электронного документооборота с использованием ЭЦП согласно Директиве и украинского законодательства.

1. *Мелащенко А.О.*, *Перевозчикова О.Л.* Організація кваліфікованої інфраструктури відкритих ключів. – К.: Наукова думка, 2010.
2. *ISO/IEC* 29500:2008 Information technology – Document description and processing languages – Office Open XML File Formats.
3. *ISO/IEC* 26300:2010 Information technology – Open Document Format for Office Applications (OpenDocument), v1.2.
4. *ISO/TS* 15000 Electronic business eXtensible Markup Language (ebXML).
5. *ISO/IEC* 9594-8:2008 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
6. *ДСТУ* EN 14890:2011 Прикладний інтерфейс для смарт-карток, використовуваних як безпечні засоби створення підписів.
7. *Directive* 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
8. *Закон* України «Про електронний цифровий підпис» від 22.05.2003, № 852.
9. *Закон* України «Про електронні документи та електронний документообіг» від 22.05.2003, № 851.
10. *Мелащенко А.О.*, *Свиридов Є.О.* Комп'ютерна програма «Бібліотека функцій криптографічних перетворень «UPGCryptoProviderBasic» // Свідоцтво про реєстрацію авторського права на твір № 31086 від 24.11.2009

Получено 01.06.2011

Об авторе:

Мелащенко Андрей Олегович,
кандидат физико-математических наук,
научный сотрудник.

Место работы автора:

Институт кибернетики
им. В.М. Глушкова НАН Украины,
проспект академика Глушкова, 40.
Тел.: 526 3603.
dep145@gmail.com