УДК 681.3:002.651.028(083.73)

А.О. Мелащенко

ЗАДЕЙСТВОВАНИЕ КВАЛИФИЦИРОВАННОЙ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ В УКРАИНЕ

В статье аргументирован подход к построению Национальной системы электронных цифровых подписей на основе нормативной базы Евросоюза. Описаны бизнес-алгоритмы, использующие электронную цифровую подпись как «якорь» доверия. Проанализирован уровень интеграции электронной цифровой подписи, основанной на нормативной базе Евросоюза, в современные офисные пакеты, как базовые инструменты обслуживания электронных бизнесов.

Введение

Согласно «Стратегии для инновационного и интегрированного европейского информационного общества» [1]: «i2010 стратегия объединяет политику, инициативы и действия Евросоюза для развития и использования ИКТ-технологий в повседневной жизни. ИКТ – способствуют экономическому росту, созданию новых рабочих мест и повышению качества жизни. i2010 – часть Лиссабонской стратегии, цель которой – модифицировать экономику Европу в направлении динамического управления знаниями и повышения конкурентоспособности». В рамках этой стратегии развилась квалифицированная инфраструктура открытых ключей (QPKI), целью которой является «установление доверия к е-транзакциям/е-услугам» [2]. QPKI – набор аппаратных средств, программного обеспечения, людей, политик и процедур, соответствующих Директиве 1999/93/ЕС и необходимых для создания, управления, распространения, использования, хранения и аннулирования усиленных сертификатов открытых ключей.

Развивает стратегию i2010 «План развития цифровой Европы» [3], представленный на конференции ICT 2010 [4].

Юридическая правомочность электронная цифровая подпись (ЭЦП) поддерживается национальным законодательством. Закон Украины об ЭЦП [5] реализует Директиву [6] (далее Директива), достигая юридического признания ЭЦП на европейском уровне. Это вытекает из требований Закона Украины [5] и Директивы [6], которые приравнивают ЭЦП к рукописной подписи (таблица). Отметим, что Еврокомиссия позитивно оценила реализацию Директивы в законодательстве Украины.

Закон Украины [5] и Директива [6] реализуют квалифицированную подпись, как ЭЦП (ст. 1 Закона Украины [5]), основанную на усиленном сертификате и надежном средстве создания подписи (SSCD). Новация подхода Директивы [6] заключается в регламентации отдельных требований и процедур сертификации органов сертификации, издающих усиленные сертификаты и производителей SSCD. Наличие сертификации гарантирует качество услуг, в том числе уровень доверия к поставщикам услуг ЭЦП и юридическую эквивалентность квалифицированных ЭЦП в рамках ЕС. Поскольку Закон Украины [5] реализует бизнес-процессы Директивы, целесообразно организовать работу национальной системы ЭЦП (НСЭЦП) в соответствии с европейской организационно-технологической базой.

Второй важный аспект (ЭЦП) – нормативно-правовая база, регламентирующая работу НСЭЦП. Целесообразно разработать Технический регламент НСЭЦП как инструмент, регламентирующий реализацию всех положений Закона Украины [6] через конкретные технологии, изложенные как национальные стандарты. Этот подход находится в полном соответствии с «новым подходом», заложенным в Директиве и нацеленным на выполнение положений законов через конкретные нормы и требования стандартов. Целесообразна и обратная связь, когда нарушение конкретной нормы стандарта влечет за собой нарушения законодательства.

Таблица. Сравнение терминологии ЭЦП

Ст. 3 Закон Украины «Про электронную цифровую подпись»	Ст. 5 Директива 1999/93/ЕС	Соответствие
Электронная цифровая подпись по правовому статусу приравнивается к рукописной подписи (печати) в случае, если:	а) удовлетворяли юридическим требованиям к подписи относительно данных, поданных в электронной форме, равно рукописная подпись …	+
электронная цифровая подпись подтверждена с использованием усиленного сертификата ключа с помощью надежных средств цифровой подписи	… созданные с помощью безопасных механизмов создания подписи:	+
при проверке использован усиленный сертификат ключа, действующий на момент наложения электронной цифровой подписи	Государства-участники обеспечивают расширенные электронные подписи, основанные на усиленных сертификатах	+
личный ключ подписанта соответствует открытому ключу, указанному в сертификате	–	–
Электронная подпись не может быть признана недействительной только из-за электронной формы или не базируется на усиленном сертификате ключа	Государства-участники обеспечивают невозможность лишения подписи юридической силы и приемлемости в качестве доказательства в судопроизводстве лишь на том основании, что она: - выполнена в электронной форме, или - не основана на действующем сертификате, или - не основана на действующем сертификате, выданном аккредитованным органом сертификации, или - не наложена с помощью безопасного механизма создания подписи.	+

Третьим важным аспектом ЭЦП является реализация QPKI как технологии, гарантирующая приведение НСЭЦП к открытой системе [7, 8].

Цель работы – описать бизнес-процессы eCommerce и предложить инструментарий их поддержки, проанализировать уровень интеграции элементов QPKI в инструменты.

1. Экономические аспекты задействования ЭЦП

Выгоды. Построение систем на основе ЭЦП целесообразно ввиду существенных экономических выгоды для всех участников рынка (государства, граждан и бизнеса).

1. Выгоды государства:

1.1. Полный контроль над всеми подвластными сферами, в частности фискальной отчетностью посредством реализации электронного документооборота, минимизирующего человеческий фактор в искажении информации, значительно ускоряющего ее обработку и допускающего использования OLAP и DataMining.

1.2. Снижает издержки на содержание государственного аппарата, оптимизируя и автоматизируя процессы в рамках органов власти, также предоставляет возможность гражданам продуктивнее сотрудничать с государством, посредством электронных государственных услуг (например, выдача справок, регистрация запросов и т. п.).

1.3. ЭЦП составляет основу электронного правительства.

2. Выгоды граждан:

2.1. Государственные электронные услуги.

2.2. Безналичный расчет за услуги общественного транспорта, eBanking, электронная демократия и т. п.

3. Выгоды бизнеса:

3.1. За счет электронного документооборота.

3.1.1. Ускорение оборота средств.

3.1.2. Автоматизации построения и сдачи фискальной отчетности.

3.1.3. Упрощение процедур согласования.

3.1.4. Улучшение контроля над ресурсами предприятия.

3.1.5. Сокращение накладных расходов.

3.2. За счет eCommerce.

3.2.1. Упрощение поиска новых рынков сбыта.

3.2.2. Упрощение поиска новых сырьевых рынков.

3.2.3. Упрощение интеграции с системами партнеров и клиентов.

Вопрос гарантий вынесен за рамки выгод он требует особого внимания, поскольку является основой доверия электронных бизнесов, в частности eCommerce.

Гарантии. Экономические выгоды являются необходимым, но не достаточным условием успешного внедрения ИТ на основе ЭЦП. Рассмотрим украинское законодательство с позиций обязательств и обязанностей сторон: регулятора (государства) и потребителей (граждан/бизнеса).

Ст. 8 Закона Украины [5] регламентирует обязанности государства в сфере ЭЦП, в частности:

1) обеспечивать защиту информации в автоматизированных системах согласно законодательству;

2) обеспечивать защиту персональных данных, полученных от подписчика, согласно законодательству;

3) обеспечивать круглосуточный доступ пользователей к сертификатам ключей и соответствующим регистрам сертификатов через телекоммуникационные каналы общего пользования;

4) предоставлять консультации по вопросам, связанным с электронной цифровой подписью.

Пункты 1) и 2) поддерживаются нормативной базой информационной безопасности, не соответствующей международным стандартам оценки и организации IT-безопасности. Этот факт не способствует признанию НСЭЦП международным сообществом.

Пункт 3) требует наличия в стране сертифицированных провайдеров телекоммуникационных услуг, гарантирующих наличие канала 24/7. К сожалению, в меру исторических факторов в стране качество телекоммуникаций крайне низкое.

Пункт 4) сложен для фактической реализации, поскольку в настоящее время в стране не создана база для обучения разного рода специалистов по внедрению, поддержке и пользованию услугами ЭЦП.

Гарантии физического и юридического лица. Отметим наличие специфики электронной подписи в том, что она не может быть обезличена и привязана к конкретному физическому лицу.

Подписант обязан (ст. 7 Закона Украины [5]):

1) сохранять личный ключ в тайне;

2) предоставлять центру сертификации ключей данные согласно требованиям статьи 6 этого Закона для засвидетельствования действия открытого ключа;

3) своевременно предоставлять центру сертификации ключей информацию об изменении данных, отображенных в своем сертификате ключа.

Выполнение требований п. 1) – нетривиальная задача, не всегда подконтрольная подписанту, поскольку Закон Украины не требует сохранения личного ключа на аппаратном носителе (токены, смарт-карточки) (далее токены), а допускает программные (файлы) и программно-аппаратные средства (флешки, диски). Задействование токенов позволяет гарантировать владение и защиту личного ключа, через физическое владение им, поскольку личный ключ защищён аппаратными средствами. При задействовании программных и программно-аппаратных средств личный ключ обрабатывается в оперативной памяти компьютера, к которой можно получить доступ и извлечь личный ключ.

Также слаб пункт 3), поскольку облегчает путь злоумышленнику, посредством использования ключа пропавшего безвести человека на протяжении срока валидности ключа. Проблемы такого рода связаны со слабой информационной интеграцией служб государства в целом.

2. Бизнес-процессы, использующие QPKI

В настоящее время НСЭЦП используется в целях сдачи фискальной отчетности, широкого применения в бизнесе она не приобрела по ряду причин:

1. Отсутствие интеграции с распространенными офисными пакетами MS Office и OpenOffice.org.
2. Отсутствие интеграции с популярными почтовыми клиентами MS Outlook, MS Outlook Express, The Bat, Mozilla Thunderbird, Evolution, Kmail.
3. Потребность в значительных капиталовложениях для интеграции в существующие системы.
4. Слабая стандартизация организационных и технических составляющих.
5. Проблемы кросссертификации.

Все указанные проблемы связаны с отсутствием интероперабельности НСЭЦП [8].

На современном предприятии основными инструментами офисных работников являются:

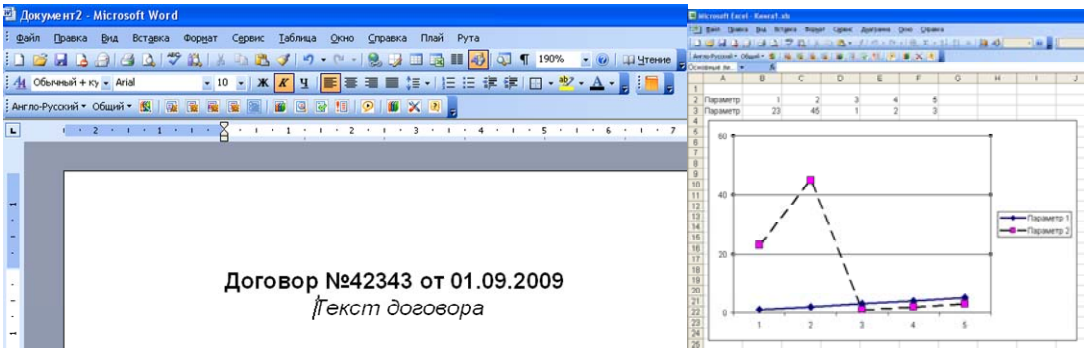
1) Текстовый процессор (например, MS Word 2010);

2) Процессор электронных таблиц (например, MS Excel 2010);

3) Почтовый клиент (например, MS Outlook 2010).

Отдельно выделим государственную фискальную отчетность, которая сдается в текстовом формате либо в формате XML. Текстовый формат наиболее характерен для банковской системы, но вступление Украины в всемирную торговую организацию требует приведения фискальной отчетности НБУ к международным нормам, точнее полной переработки существующей системы и программного обеспечения (ПО) [9]. А последние версии офисных пакетов используют формат XML.

Оформление документа. Любой договор, счет, отчет и т. п. можно представить в текстовых процессорах и/или процессорах электронных таблиц (рис. 1).



а) б)

Рис. 1. Примеры документов

Бизнес-процесс получения услуги выглядит как на рис. 2. Здесь схема имеет такие недостатки.

– для каждого действия, как правило, требуется отдельный исполнитель;

– на этапе запроса/предложения в реальной жизни люди опираются на «честное слово», но при заключении «крупных» сделок требуется финансовые или письменные подтверждения;

– при интенсивном документопотоке трудно отслеживать и стыковать документы;

– проблемы хранения, учета и т. п.

При использовании ЭЦП этот бизнес-процесс упростится посредством (рис. 3):

– четкого описания документопотоков;

– автоматической регистрации документов;

– автоматической доставки исполнителям;

– автоматической «стыковки» документов;

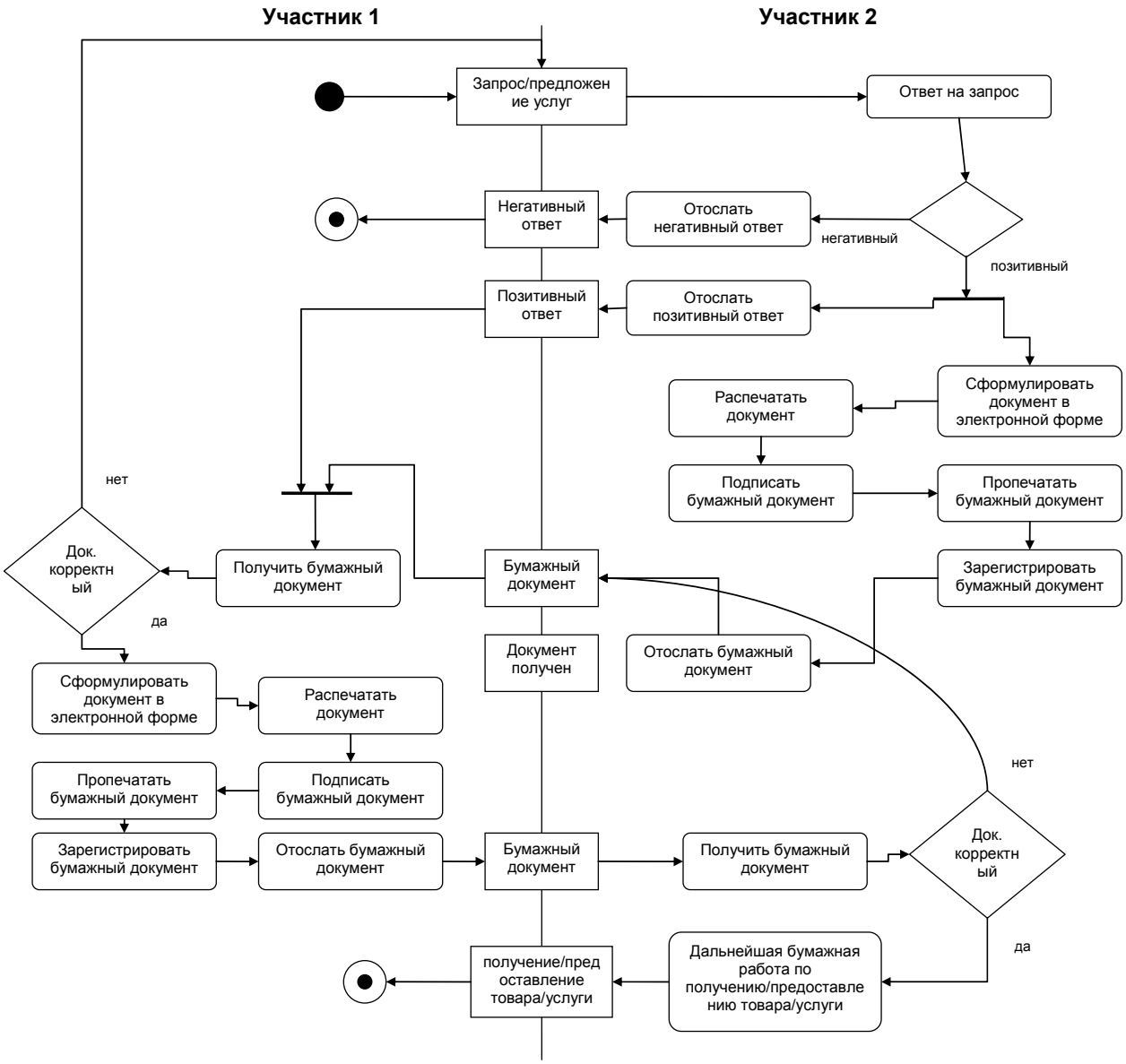


Рис. 2. Типичный бизнес-процесс получения/заказа услуг/товаров

– юридической валидности всех обменов и документов;

– экономии бумаги;

– упрощения хранения;

– удаления этапов печати документов;

– повышения исполнительной дисциплины.

Типичная договоренность. Под договоренностью имеем ввиду этапы запроса продукта/услуги, согласований, утверждений и т. п. Как правило, договариваются устно или письменно; рассмотрим письменный вариант, а именно электронную почту (рис. 3).

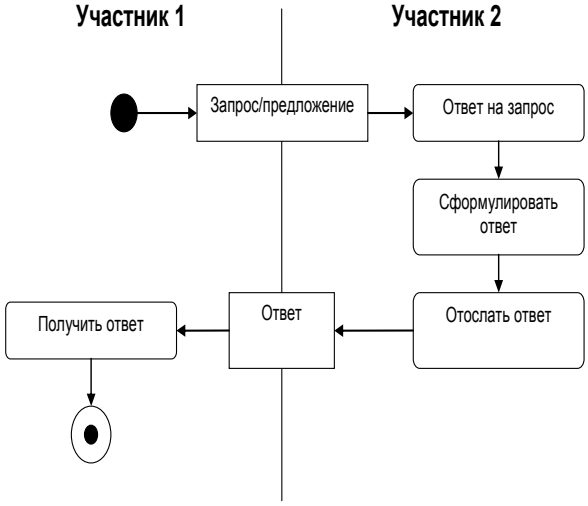


Рис. 3. Типичный бизнес-процесс договоренности

Передача XML-документа. Наилучшим примером является налоговая фискальная отчетность в Украине. Имеем некий формат XML-документа, который надо передать, гарантируя целостность и аутентичность. Существует два способа с использованием:

– встроенной подписи для XML-документов, XAdES [10] (рис. 4);

– оберточного формата, например CAdES [11] (рис. 5).

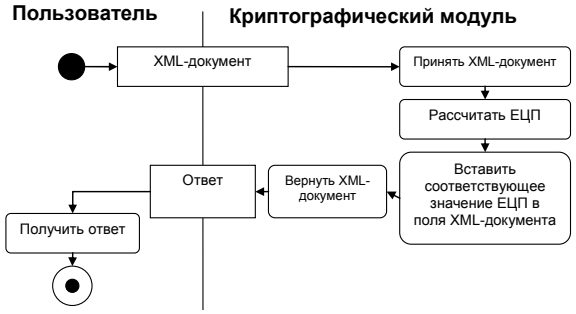


Рис. 4. Типичный бизнес-процесс подписания документа, используя XML Signature

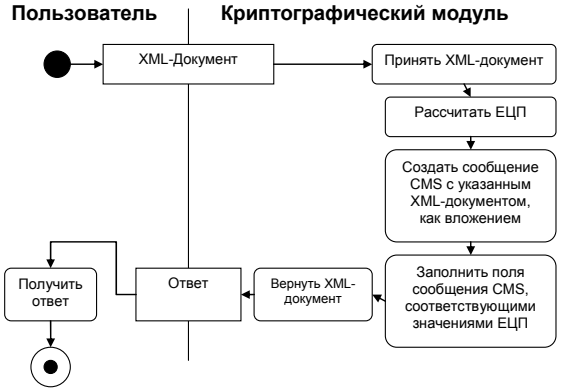


Рис. 5. Типичный бизнес-процесс подписания документа, используя CMS

3 Внедрение и использование QPKI

Для полноценного функционирования QPKI необходимы:

1. Органы сертификации (CA или в Украине ЦСК), содержащие модули:

а) генерации пары открытого и личного ключей;

б) издания усиленных сертификатов;

в) генерации списков аннулированных сертификатов;

г) регистрации и т. п.

2. Клиентское программное обеспечение (ПО) наложения ЭЦП на документ/сообщение.

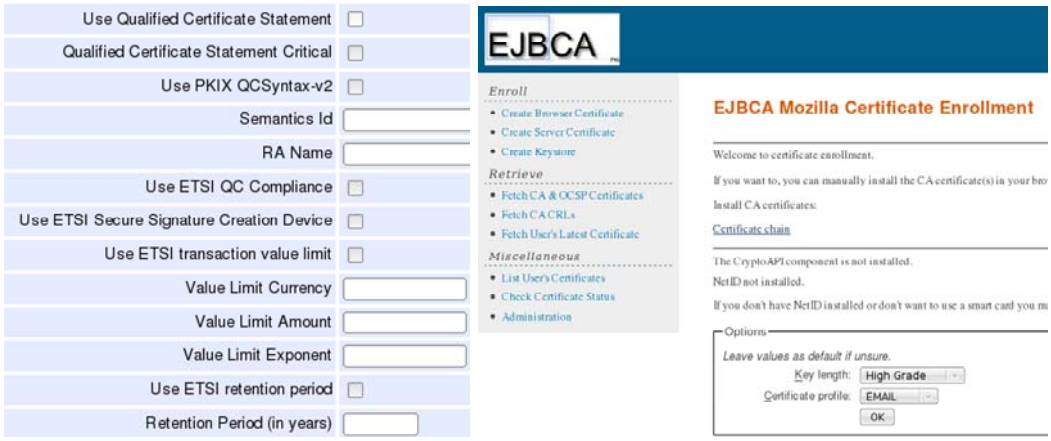
Надежная система органа сертификации. Рассмотрим две альтернативные системы, EJBCA как надежную и стабильную систему, используемую многими государствами ЕС [12], и Услуги сертификации для Active Directory Windows server 2008, как наиболее распространенную систему.

EJBCA (рис. 6) – надежная система CA, построенная на основе технологии Java для предприятий (J2EE – Java Platform, Enterprise Edition) [13]. Этот инструментарий активно используют государственные органы Франции, Швейцарии, Испании и множество организаций во всей Европе. Максимальное количество известных пользователей одной инсталляции достигает 100 000. Эта система CA поддерживает QPKI [8].

Система работает с аппаратными и программными генераторами ключей, токенами, поддерживает удаленное обновление ключа, работает на множестве платформ и различном ПО, легко масштабируется, поддерживает разные информационные хранилища, СУБД и LDAP.

Услуги сертификации для Active Directory Windows server 2008. Windows недостаточно удобен для развертывания QPKI. К сожалению, Microsoft не реализовала поддержку QPKI, ввиду чего невозможно быстро и «безболезненно» развернуть QPKI. Причем компетентным органам Украины вице-президент Microsoft Steve Ballmer передал исходные коды модуля политик безопасности для Windows. Наличие исходных кодов позволяет реализовать любые политики, в том числе и европейские, поэтому уместен вопрос о приведении существующих политик безопасности к европейскому уровню и включении их в поставку украинского дистрибутива Windows.

ПО пользователя. Обычно пользователи используют стандартное ПО: MS Office, OpenOffice, поддерживающие XML-документы в форматах OpenXML [14] и ODF [15], они поддерживают XAdES [10]. Продемонстрируем работу стандартного ПО пользователя и сертификата, созданного с помощью EJBCA для гарантии аутентичности и целостности документов и электронных писем.



а) б)

Рис. 6. Примеры: а – профиля сертификата, б – запроса сертификата

Перед началом эксперимента импортируем сертификат, используя стандартные инструменты операционной среды Windows в систему управления сертификатами компьютера.

Офисные пакеты. На рис. 1, показаны примеры офисных документов, которые необходимо защитить от несанкционированного изменения и идентифицировать их исполнителей. Также эти документы реализуют и поддерживают бизнес-процесс, указанный на рис. 2. При создании документа исполнитель накладывает ЭЦП (используя стандартный механизм офисного пакета) и отсылает по электронной почте документ адресату в соответствии с документопотоком.

Почтовые клиенты. Большинство популярных почтовых клиентов имеют встроенные механизмы подписания сообщений, используя стандартный формат S/MIME [16] (рис. 7), который не поддерживает в полной мере формат подписи CAdES [11]. Несмотря на слабую поддержку формата CAdES, в Приложении F [11] предложена процедура использования CAdES в S/MIME.

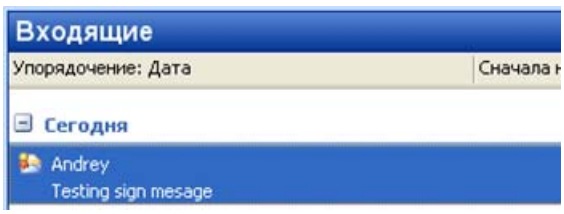


Рис. 7. Пример подписанного сообщения

На сегодня можно использовать усиленные сертификаты для подписания почтовых сообщений, реализуя бизнес-процесс, показанный на рис. 3.

Подписание XML-документов. Как показано на рис. 4 и 5, можно встроить или «обернуть» подписание XML документа. В первом случае используются процедуры подписания, изложенные в XAdES [10], во втором – CAdES [11].

Мировая практика для целей фискальной отчетности и функционирования бизнеса в целом использует стандартные форматы XML-документов (например, XBRL [17], ebXML [18]), в которых встроены функции ЭЦП.

Выводы

Рассмотрены базовые бизнес-процесс и юридические, технические и организационные вопросы, связанные с внедрением QPKI в Украине. Поддерживающие QPKI разработки интегрированы в офисные пакеты, как основные инструменты пользователей ЭЦП.

Для полноценного использования ЭЦП необходимо привести НСЭЦП к открытой системе, разработав Технический регламент НСЭЦП.

Стоит отметить важность и срочность работы по приведению модулей безопасности MS Windows к европейским нормам и стандартам, без которых развертывание QPKI в Украине значительно усложнится.

В работе показано наличие готовых решений для надежных систем органов сертификации и практически полную поддержку функций ЭЦП в популярных офисных приложениях, что гарантирует надежное и быстрое развертывание QPKI в Украине. Это позволит в кратчайшие сроки получить экономический эффект. Однако без дальнейшего совершенствования законодательства, в частности в сферах НДС, электронной идентификации, тендерных закупок, eCommerce, банковской сфере и т. п., и приведения ИТ безопасности к мировым нормам и стандартам, невозможно полно раскрыть потенциал QPKI и интеграции Украины в ВТО.

1. *Strategy* for an innovative and inclusive European Information Society, апрель 2004. http://ec.europa.eu/information_society/eeurope/i2010/strategy/index_en.htm
2. *Study* on the standardisation aspects of eSignature, 22.11.2007. http://www.esstandardisation.eu/
3. *Communication* from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. A Digital Agenda for Europe COM/2010/0245 f/2
4. *ICT* 2010 http://ec.europa.eu/information_society/events/ict/2010/index_en.htm
5. *Закон України* «Про електронний цифровий підпис» № 852 від 22.05.2003.
6. *Directive* 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
7. *Мелащенко А.О., Перевозчикова О.Л.* Национальная система электронных цифровых подписей как открытая система //Кибернетика и системный анализ. – 2011. – № 3. – С. 31–39.
8. *Мелащенко А.О., Перевозчикова О.Л.* Організація кваліфікованої інфраструктури відкритих ключів. – К.: Наукова думка, 2010. – С. 3–4.
9. *Мелащенко А.О., Перевозчикова О.Л., Стрельникова Ж.А.* Онтологии финансово-экономического информационного хранилища // Проблеми програмування. – 2010. – № 1. – С. 419–428.
10. *ДСТУ* ETSI TS 101 903:2009. XML-розширені електронні підписи (XAdES).
11. *ДСТУ* ETSI TS 101 733:2009. Електронні підписи та інфраструктури (ESI). CMS-розширені електронні підписи (CAdES)
12. *EJBCA*. http://ejbca.sourceforge.net/
13. *J2EE*. http://java.sun.com/javaee/index.jsp
14. *ISO/IEC* 29500:2008. Information technology – Office Open XML file formats
15. *ISO/IEC* 26300:2006. Information technology – Open Document Format for Office Applications (OpenDocument)
16. *RFC* 3851. «Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1. Message Specification», 2004.
17. *eXtensible* business reporting language (XBRL), 2008. http://www.xbrl.org
18. *ISO/TS* 15000. Electronic business eXtensible Markup Language (ebXML).

Получено 31.03.2011

Об авторе:

Мелащенко Андрей Олегович,
науковий співробітник .

Место работы автора:

Институт кибернетики имени В.М. Глушкова НАН Украины.
03187, Киев-187,
проспект Академика Глушкова, 40.
Тел.: 526 3603.
dep145@gmail.com