СИСТЕМНЫЙ АНАЛИЗ

А.О. МЕЛАЩЕНКО, О.Л. ПЕРЕВОЗЧИКОВА

УДК 681.3:002.651.028(083.73)

ПРОБЛЕМЫ ИНТЕРОПЕРАБЕЛЬНОСТИ НАЦИОНАЛЬНОЙ СИСТЕМЫ ЭЛЕКТРОННЫХ ЦИФРОВЫХ ПОДПИСЕЙ

Ключевые слова: *электронная цифровая подпись, интероперабельность, гармонизация стандартов, криптографический алгоритм (криптоалгоритм), валидация, верификация, политика подписания*.

ВВЕДЕНИЕ

Национальная система электронных цифровых подписей (ЭЦП) Украины, функционирующая с июля 2005 года, от имени государства гарантирует качество услуг ЭЦП, а Центральный удостоверяющий орган (укр. Центральний засвідчувальний орган — ЦЗО) регулирует их качество, являясь органом аккредитации и государственного надзора за деятельностью центров сертификации ключей (ЦСК), аккредитованных и зарегистрированных. На май 2009 года аккредитовано десять ЦСК, насчитывающих более полумиллиона клиентов.

В настоящее время Национальная система ЭЦП по организационным причинам не интероперабельна преимущественно из-за слабой координации действий ЦЗО и контролирующего органа как главных субъектов Закона Украины об ЭЦП от 22.05.2003 №852, гармонизированного с Директивой Евросоюза 1999/93/ЕС, а также ввиду существенных пробелов в законодательной базе [1–14] и технологических просчетов в реализации информационных технологий (ИТ), поддерживающих функционирование ЦЗО и всех ЦСК. Основное препятствие обусловлено хуторянской позицией Украины, т.е. ориентацией на негармонизированный национальный стандарт ДСТУ 4145 и СНГ-стандарты ГОСТ 34.310 и ГОСТ 34.311, а не на международные ЭЦП согласно действующим гармонизированным стандартам ДСТУ ISO/IEC 14888:2002, ДСТУ ISO/IEC 13888:2002, ISO/IEC 9798:2002, ДСТУ ISO/IEC 10118:2003, ДСТУ ISO 9735:2006, ДСТУ ISO/IEC 18014:2002. Даты утверждения этих ДСТУ в 2002 и 2006 гг. однозначно негативно характеризуют организационно-технологическое влияние контролирующего органа на развертывание всей Национальной системы ЭЦП в Украине.

Проблемы интероперабельности Национальной системы ЭЦП привели к значительному сужению круга пользователей ЭЦП и способствовали отрицательному имиджу у инвесторов в отличие от ЕС, в котором от грамотного регулирования ЭЦП зависят не только сферы электронного бизнеса (eHealth, eTransport, eCommerce, eGovernment, eInvoicing, eProcurement), но и поддержка всех функций информационного общества. По этой причине представляется незначительным экономический эффект от внедрения в Украине электронного документооборота, основанного на ЭЦП. Определенной части этого эффекта можно достичь вследствие интеграции Украины в СОТ, что невозможно для электронного бизнеса без кроссертификации, т.е. трансграничного признания сертификатов открытых ключей ЭЦП, изданных в разных странах. Согласно Закону Украины об ЭЦП право на кроссертификацию имеет ЦЗО, но он к этому не готов. В процедурах кроссертификации, в частности с ЕС, предусмотрены

полномасштабная валидация и автоматическое Интернет-тестирование всей Национальной системы ЭЦП, а также анализ ее законодательной базы.

Цель статьи — обосновать способы минимаксного (минимум затрат, максимум результатов) решения проблем интероперабельности в инфраструктуре ЭЦП как внутри Украины, так и с другими государствами.

ТЕКУЩЕЕ СОСТОЯНИЕ НАЦИОНАЛЬНОЙ СИСТЕМЫ ЭЦП

Согласно европейской бизнес-модели ЭЦП [1] существуют три вида так называемых квалифицированных подписей, поэтому соответствующую инфраструктуру ЭЦП называют QPKI в отличие от принятой за пределами Евросоюза PKI (инфраструктура открытых ключей X.509) [14].

1. **Параллельные** подписи – взаимно независимые подписи, когда не важен порядок наложения подписей на документ и их можно создать независимо одна от другой. Независимые подписи применяют только к хешу данных (контенту документа).

2. **Последовательные** подписи суть разновидности параллельных подписей, но порядок подписей имеет значение. Последовательные подписи можно применить к одному контенту данных, а также добавлять к нему другие подписи, но только как часть контента данных; они не заменяют контрподписи или вложенные подписи и полезны для управления множественными подписями в потоке данных или документов.

3. **Вложенные** подписи задают сценарий, когда одна подпись применена к другой, т.е. одна вложена в другую. Последовательность применения подписей важна ввиду наличия между ними взаимосвязи, валидность первой подписи зависит от второй. Например, существует требование засвидетельствования ЭЦП другим человеком: первичная подпись поставлена, т.е. контрподпись применена непосредственно к первой (вложенная подпись). Эти подписи необходимы, когда одна из функций второй подписи должна удостоверить прием документа с первой подписью. Кроме того, контрподпись может также удостоверить независимо либо в комбинации: а) верификацию или одобрение семантики данных, изначально подписанных; б) валидацию идентичности первичной подписи; в) верификацию валидности первичной подписи (возможно, с верификацией валидности сертификата или согласно политике подписания).

Помимо трех типов подписи, ЭЦП еще различают по требованию непосредственного участия человека в процессе подписания электронного документа. Например, для выставления счета на товары в виртуальном магазине не требуется вмешательства человека в процесс подписания (кроме этапа конфигурирования), но согласно Закону Украины об ЭЦП [2] недопустимо автоматическое подписание электронных документов без участия человека. А юрисдикции большинства государств ЕС допускают такой сценарий манипулирования ЭЦП. К сожалению, в Украине нет четкого разграничения понятий *печать* и *штемпель*, поэтому сложно, а порой и невозможно однозначно интерпретировать их электронное значение.

Построить полноценные бизнес-модели ЭЦП невозможно без обязательного атрибута подписи — временного штемпеля и/или маркера времени. Маркер времени — информация в следе аудита провайдера надежных услуг, связывающая представление данных с конкретным временем и являющаяся доказательством, что данные существовали до этого времени. Токен временного штемпеля — аналогичный объект данных в контейнере ЭЦП и/или подписанного документа. В Украине отсутствует техническое регулирование этой составляющей Национальной системы ЭЦП, несмотря на наличие с июля 2008 года в Институте метрологии (г. Харьков) доступного в Интернете сервера времени, функционирующего согласно требованиям эталонного времени Международного телекоммуникационного радиокомитета ITU-R и бюро контроля времени BIPM, 200 атомных часов которого размещены в лабораториях и обсерваториях 30 стран (ftp://62.161.69.5/pub/tai/publication). На харьковском сервере легко построить надежную инфраструктуру штемпелевания времени любого отдельного органа или составляющей ЦСК [3–4].

В поддержку трех типов подписи разработаны форматы подписей. Ниже перечислены основные из них:

— базовая электронная XML-подпись (XAdES-BES) [5];

— XML-ЭЦП, основанная на явной политике подписания (XAdES-EPES) [5];

— XML-ЭЦП с данными валидации (XAdES-T и XAdES-C) [5];

— базовая подпись CAdES (CAdES-BES) [6];
— подпись CAdES, основанная на явной политике подписания (CAdES-EPES) [6];
— подпись со временем (CAdES-T) [6];
— подпись со ссылками на полные данные валидации (CAdES-C) [6].

Форматы подписи как контейнеры с конкретными наборами атрибутов определены в [5, 6]. Используя эти атрибуты, можно создать произвольные форматы ЭЦП на основе стандартных или полностью независимых.

В настоящее время в Украине реализована только одна, простейшая и неинтероперабельная модель подписи [1], а полноценная бизнес-модель ЭЦП поддерживается тремя составляющими: политика подписания, профиль, комплект подписи.

1. Политика подписания — набор правил для создания и валидации ЭЦП; под политикой ЭЦП считается валидной в конкретном контексте транзакций. Политику подписания можно задать, используя такую формальную нотацию, как ASN.1, или в неформальной свободной текстовой форме, т.е. задавая точно специфицированные правила политики. Когда две или более сторон взаимодействуют в электронной бизнес-среде, они должны определить условия, при которых можно использовать ЭЦП. Политика подписания определяет сферу применения и использования ЭЦП для соответствия условиям контекста каждой транзакции.

Таблица 1

Номер и название стандарта	Информация о регистрации на получение OID
CWA 14169:2004 Безопасные средства создания подписей «EAL 4+»	EAL 4+BSI-PP-0004-2002 Профиль защиты. Безопасные средства создания подписей типа 1. Версия 1.05 EAL 4+BSI-PP-0005-2002 Профиль защиты. Безопасные средства создания подписей типа 2. Версия 1.04 EAL 4+BSI-PP-0006-2002 Профиль зашиты. Безопасные средства создания подписей типа 3. Версия 1.05
CWA 14890:2004 Прикладной интерфейс для смарт-карточек, используемых как безопасные средства создания подписей. Часть 1. Основные требования	Важные AlgID для использования с ESIGN-приложением для функций цифровой подписи и аутентификации ESIGN-средства
CWA 14890:2004 Прикладной интерфейс для смарт-карточек, используемых как безопасные средства создания подписей. Часть 2. Дополнительные свойства	Правила кодирования OID криптоалгоритма на смарт-карточке
CWA 14167-2:2004 Криптографический модуль для операций подписания CSP с резервированием. Часть 2. Профиль защиты CMCSOB	Профиль защиты CMCSOB криптомодуля для операций подписания CSP с резервной копией (Protection Profile of Cryptographic Module for CSP Signing Operations with backup), версия 0.28. Общий статус — оценен и сертифицирован
CWA 14167-3:2004 Криптографический модуль для услуг генерации ключей провайдером услуг сертификации. Профиль защиты CMCKG-PP	Профиль защиты CMCKG-PP криптомодуля для операций подписания CSP (Protection Profile of Cryptographic Module for CSP Key Generation Services), версия 0.12. Общий статус — проект WS/E-Sign для открытых комментариев
CWA 14167-4:2004 Криптографический модуль для операций подписания CSP. Часть 4. Профиль защиты CMCSO	Профиль защиты CMCSO криптомодуля для операций подписания CSP (Protection Profile of Cryptographic Module for CSP Signing Operations), версия 0.28. Общий статус — профиль оценен и сертифицирован
ETSI TS 101 862 V1.3.3 (2006-01) Профиль усиленного сертификата	Идентификатор утверждения, созданный CA, представлен как OID из рекомендованного набора
ETSI TS 101 861 V1.3.1 (2006-01) Профиль штемпелевания времени	Профилирует RFC 3161
ETSI TS 102 734 V1.1.1 (2007-02) Электронные подписи и инфраструктуры. Профили CMS расширенных электронных подписей, основанных на TS 101 733 (CAdES)	Вводит профили для ETSI TS 102 733:· в сфере e-invocing,· в сфере e-government,· как основание для других бизнес-сфер и приложений
ETSI TS 102 904 V1.1.1 (2007-02) Электронные подписи и инфраструктуры. Профили расширенных электронных XML подписей, основанных на TS 101 903 (XAdES)	Вводит профили для ETSI TS 102 903:· в сфере e-invocing,· в сфере e-government,· как основание для других бизнес-сфер и приложений

2. Профиль. Для максимизации интероперабельности в сообществах, использующих ЭЦП в конкретных средах, необходимо идентифицировать единый набор опций, применимых в этой среде. Такой выбор обычно называют профилем и закрепляют объектным идентификатором (OID). Профили покрывают требования к надежным системам управления сертификатами, криптомодулям, безопасным средствам создания подписей и т.п. Профили — некоторый аналог отечественного Технического регламента. В табл. 1 приведен набор действующих профилей Европейского комитета стандартизации CEN/CENELEC. Отметим, что формальная процедура аккредитации специалистами ЦЗО зарегистрированных ЦСК только сейчас стала доступной вследствие принятия конкретных методик [7] оценки соответствия нормам, указанным в профилях.

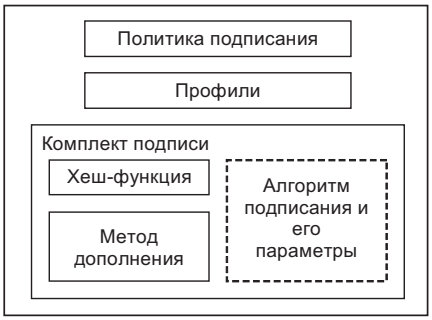

Рис. 1. Составляющие бизнес-модели ЭЦП

3. Комплект подписи. Чтобы выполнить требования безопасности и допустить подписание сообщений произвольной длины, в комплект подписи входит хеш-функция. Важно связать хеш-функцию со схемой подписания. Без этого слабейшая доступная хеш-функция может установить общий уровень защиты.

В Украине действуют стандарты на криптоалгоритмы как составляющие комплекта подписи (рис. 1). В силу возможных взаимодействий, способных повлиять на защиту ИТ, алгоритмы и параметры для безопасных ЭЦП используются только в предопределенных комбинациях, именуемых комплектами подписей. Комплект подписи состоит из трех компонентов: хеш-функции, метода дополнения, алгоритма подписания с широким набором параметров.

Если изменен один из компонентов комплекта, то его соответственно изменяют. Пример рекомендованных ETSI комплектов подписи приведен в табл. 2 [8], где использованны идентификаторы следующих компонентов комплектов:

1) sha1 (Secure Hash Algorithm 1) — алгоритм хеширования; для входного сообщения произвольной длины (максимум $2^{64} - 1$бит) алгоритм генерирует 160-битное значение хеша;

2) ripemd160 — алгоритм хеширования с длиной результата 160 бит;

Таблица 2

Имя комплекта подписи	Имя хеш-функции	Имя метода дополнения	Имя алгоритма подписания
sha1-with-rsa	sha1	Выбирается из [8]	rsa
sha1-with-dsa	sha1	Не требует дополнения	dsa
ripemd160-with-rsa	ripemd160	Выбирается из [8]	rsa
ripemd160-with-dsa	ripemd160	Не требует дополнения	dsa
sha224-with-rsa	sha224	Выбирается из [8]	rsa
sha256-with-rsa	sha256	Выбирается из [8]	rsa
rsa-pss с mgflSHA-1Identifier	mgf1SHA-1		rsa
rsa-pss с mgf1SHA-224Identifier	mgf1SHA-224		rsa
rsa-pss с mgf1SHA-256Identifier	mgf1SHA-256		rsa
sha1-with-ecdsa	sha1	Не требует дополнения	ecdsa-Fp или ecdsa-F2m
sha1-with-ecgdsa	sha1	Не требует дополнения	ecgdsa-Fp или ecgdsa-F2m
sha224-with-ecdsa	sha224	Не требует дополнения	ecdsa-Fp или ecdsa-F2m
sha256-with-ecdsa	sha256	Не требует дополнения	ecdsa-Fp или ecdsa-F2m
sha384-with-ecdsa	sha384	Не требует дополнения	ecdsa-Fp или ecdsa-F2m
sha512-with-ecdsa	sha512	Не требует дополнения	ecdsa-Fp или ecdsa-F2m
ecdsa-with-RIPEMD160	ripemd160	Не требует дополнения	ecdsa-Fp или ecdsa-F2m

3) sha224, sha256 — алгоритмы хеширования; для входного сообщения произвольной длины (максимум $2^{64} - 1$ бит) генерируются 224- и 256-битные хеш-значения соответственно;

4) sha384, sha512 — алгоритмы хеширования; для входного сообщения произвольной длины (максимум $2^{128} - 1$ бит) генерируются 384- и 512-битные хеш-значения;

5) dsa (Digital Signature Algorithm) — криптоалгоритм для создания ЭЦП;

6) rsa (Rivest, Shamir и Adleman) — криптоалгоритм для создания ЭЦП и шифрования;

7) ecdsa (Elliptic Curve Digital Signature Algorithm), ecgdsa (Elliptic Curve German Digital Signature Algorithm) — криптоалгоритмы для создания ЭЦП, определенные над полем точек эллиптической кривой.

С комплектом подписи ассоциированы рекомендованные сроки стойкости комплекта.

QPKI-ИНФРАСТРУКТУРА КВАЛИФИЦИРОВАННЫХ ПОДПИСЕЙ

Вступление Украины в СОТ и ее стремление к евроинтеграции требует скорейшей и качественной модификации Национальной системы ЭЦП, что возможно при соблюдении трех принципов: 1) модульности, 2) развития инфраструктуры независимых оценщиков, 3) внедрения Технического регламента, наделяющего поддерживающие его стандарты статусом не добровольного использования (что имеет место в настоящее время), а обязательного.

Принцип модульности. В интероперабельной QPKI модульность задействована на всех уровнях, начиная с уровня органов (сертификации, штемпелевания времени, трастовых услуг) и заканчивая уровнем криптомодулей. Модульность дает возможность органам и специализированным центрам развивать составляющие, компоненты и всю QPKI в целом, ввиду чего установлены наборы требований для компонентов и механизмов взаимодействия. Без высокоуровневой трактовки сложно достичь гибкости всей системы, а без механизмов взаимодействия — специализации отдельных групп компонентов и сущностей.

В Украине не реализован принцип модульности, а ЦСК и их пользователи применяют разработанные «под ключ» системы, не преследующие идеологию комплектов подписей [8].

Инфраструктура независимых оценщиков компонентов и сущностей QPKI. Ввиду высокоуровневого описания правил и требований к конкретным составляющим QPKI необходимо оценивать соответствие конкретного объекта относительно набора правил и, более того, реализации программно-технических комплексов (ПТК) и отдельных модулей ранжировать, например, по уровню интероперабельности.

Инфраструктура независимых оценщиков с учетом принципа модульности (рис. 2) контролирует качество каждого компонента и в целом ПТК (набора модулей для предоставления услуг). В Украине введено обязательное оценивание криптомодулей совместно с использованными хеш-функциями (http://dstszi.gov.ua), но его уровень неоправданно низок. Это отражает содержание выдаваемых сертификатов оценивания, в которых не всегда указано соответствие стандартам и цель использования криптомодуля (выдача усиленных сертификатов, штемпелевание времени, публикация статуса сертификатов и т.п.).

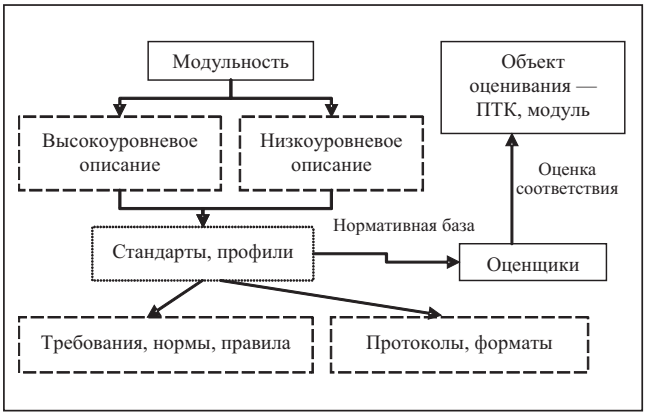

Рис. 2. Общая схема обеспечения интероперабельности QPKI

Проблемы интероперабельности Национальной системы ЭЦП обусловило различие между криптоалгоритмом, описанным в некотором стандарте, и криптомодулем, реализующим криптоалгоритм. Если каждый ЦСК использует собственный криптомодуль, а не отработанное и признанное всеми «готовое решение», то расшифровка ЭЦП на документе, проведенная адресатом посредством другого модуля, закончится неудачей. Два разных криптомодуля необходимо верифицировать на полную идентичность процедур вычисления экземпляра ЭЦП, построенных на обработке случайных чисел. Не решает проблемы простое оценивание соответствия криптомодулей спецификации криптоалгоритмов относительно стандартов. Необходимо проверять криптомодули на специальном стенде, а этого не делает никто из независимых оценщиков Украины.

С такой проблемой столкнулась Налоговая администрация Украины (укр. Державна податкова адміністрація — ДПА) в организации сдачи фискальной отчетности (рис. 3). Поскольку эту отчетность не относят к конфиденциальной информации, а ЭЦП гарантирует неопровержимость и целостность электронных документов, то не нужны защищенные каналы передачи документов. Как результат отсутствия интероперабельности «Договор с ДПА» любого ЦСК помогает решать такие проблемы ДПА:

1) невозможность создания системы, базирующейся не на одном, а на множестве криптомодулей от всех ЦСК;

2) отсутствие формата подписей;

3) отсутствие средств штемпелевания времени.

На рис. 4 приведена схема обработки ЭЦП в ДПА с предварительной верификацией/валидацией. Чтобы однозначно идентифицировать, каким модулем подписан документ, необходимо использовать реестр криптомодулей от разных ЦСК и механизм идентификации этих модулей. Такой механизм опознания криптомодулей необходимо построить всем субъектам в Украине, принимающим электронные документы от своих клиентов. Проблема усугубится вследствие предоставления услуг штемпелевания времени даже для самого простого формата параллельных ЭЦП.

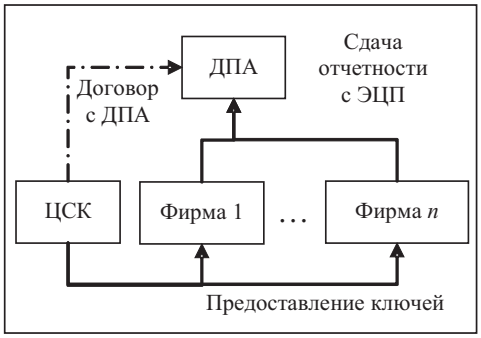

Рис. 3. Схема сдачи отчетности в ДПА

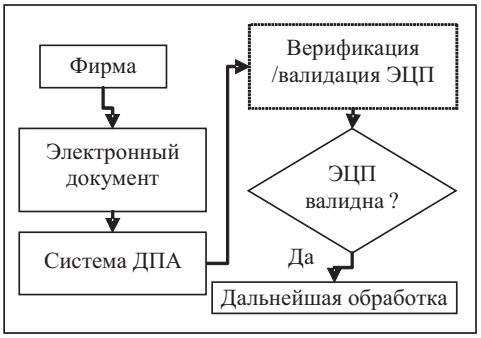

Рис. 4. Схема валидации ЭЦП в отчете фирмы

Однако и в этой схеме есть слабое звено. В процессе аккредитации нового ЦСК или при повторной аккредитации необходимо верифицировать криптомодули, задействованные в ЦСК, в отношении интероперабельного взаимодействия с ДПА клиентов этого ЦСК. Иначе говоря, в систему ДПА необходимо включить тестовый стенд, способный провести валидацию криптомодулей и других компонентов ЦСК на соответствие политике подписания ДПА. Только при наличии стенда можно гарантировать надежное обслуживание со стороны ДПА.

ОТСУТСТВИЕ ФОРМАТА ПОДПИСЕЙ

Отсутствие формата подписей привело к созданию файла «все в одном» (рис. 5), выполняющего функции [9]:

— транспортного протокола,

— контейнера отчета,

— контейнера сертификата,

— контейнера ЭЦП в отчете,

— контейнера параметров ЭЦП.

За основу взят протокол SMTP [10]. «Жесткая» нотация обменного формата привела к постоянным его пересмотрам и переработкам, что повлекло за собой ошибки как со стороны пользователей, так и систем обработки ЦСК и ДПА. Недостаток подхода — невозможность предоставления статуса обработки отчета, даже в режиме полу-онлайн. Использование электронной почты — простое, но недостаточно практичное решение, поскольку несвоевременная сдача отчета приводит к финансовым последствиям, а ответ ДПА можно получить за два часа [11].

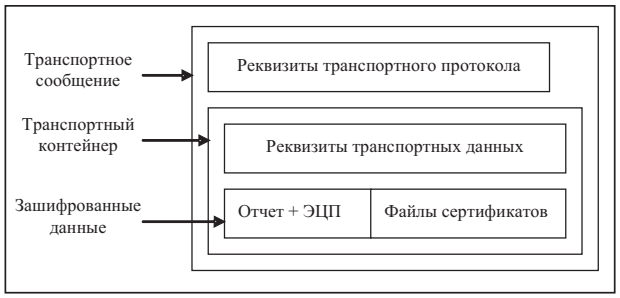

Рис. 5. Формат транспортного сообщения в ДПА

Оптимально решить эту задачу можно в два этапа:

— разделение функциональных нагрузок;

— интеграция отчета, ЭЦП и сертификатов (в будущем не только открытого ключа, но и атрибутов), а также токенов временных штемпелей/маркеров времени.

Разделение функциональных нагрузок. Согласно [12] формат отчетов ДПА имеет вид XML-документов, как современной формы обмена. Существуют разнообразные формы обмена XML-документами, например e-mail, http, ftp, webdav, soap, rest. Ограничивать их использование нецелесообразно. Более практично организовать основанное на контракте взаимодействие (веб-службы) и обеспечить обмен безопасной информацией (в XML-документах в отношении вредоносного программного продукта) и вариацию реализаций, не зависящую от конечного формата обмена. К достоинствам этого подхода отнесем простое онлайн отображение статуса отчетов в разных формах. Последнее очень важно, поскольку публикация на сайте морально устарела, а конечным пользователям не всегда удобно просматривать реестры на сайте.

Отметим, что обменный формат не должен содержать дополнительных данных об XML-документах, поскольку сами документы предоставляют минимально достаточный объем данных для обработки системами ДПА. Эти данные размещены в заголовке сообщения, содержащем перечень вложенных файлов-отчетов.

Формат подписей. Реализация сдачи отчетности организована с использованием административных рычагов, что обусловило:

1) ввод отдельных ключей для сдачи отчетности. При такой политике конечный пользователь должен иметь десятки ключей для полноценного использования услуг ЭЦП, в частности eGovernment;

2) неточность описания процесса подписания. Например, из трех наличных подписей (директора, бухгалтера, мокрой печати) неясно, какой из трех вариантов (параллельные, контрподписи, независимые) согласно [1] применим для заверения контента отчета. При смене должности директор и/или бухгалтер должны снова проходить трудоемкую процедуру сертификации открытых ключей;

3) каждый государственный орган должен придумывать свои решения по совместной передаче и/или получению данных и сертификата открытого ключа; используя его, можно сгенерировать ЭЦП с параметрами.

Пока ДПА вынужденно реализовала специфический вариант, в котором:

1) назначение ключей гарантирует отдельный тип ключей, издаваемых ЦСК;

2) процесс частично описан в договоре, заключенном между ДПА и фирмой [11];

3) утвержден собственный формат объединения данных для использования ЭЦП в ДПА.

В этой схеме много «творческих» решений, негативно зарекомендовших себя на практике, например договор, который обязаны заключить фирма и ДПА. Согласно [13] «юридическая сила электронного документа не может быть отвергнута только на основании того, что он имеет электронную форму», т.е. согласно Закону

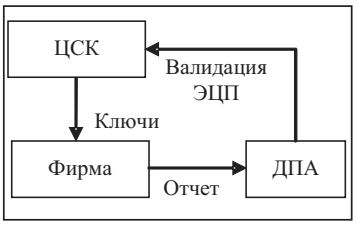

Рис. 6. Схема сдачи отчетности по законодательству

[13] реализуется схема, изображенная на рис. 6, а фактически работает схема на рис. 7. Схема на рис. 7 стала реальной ввиду отсутствия интероперабельности Национальной системы ЭЦП. В дополнение к организационно-юридической составляющей реализация транспортного сообщения стала ответом на такие технологические требования, как доступ к ЭЦП, параметрам ЭЦП, данным, сертификатам.

Попытка построить специализированную систему частично удалась. Для дальнейшего внедрения ЭЦП и получения соответствующего экономического эффекта необходимо стандартизировать все составляющие Национальной системы ЭЦП для полной интероперабельности разных систем. В общем случае необходимо использовать формат подписи и согласно [5] включить его как подсхему схемы отчетов. В стандарте [5] решена проблема дополнительных полей в транспортном протоколе и объединения необходимых данных. Верификацию организационных и юридических аспектов покрывает политика подписания.

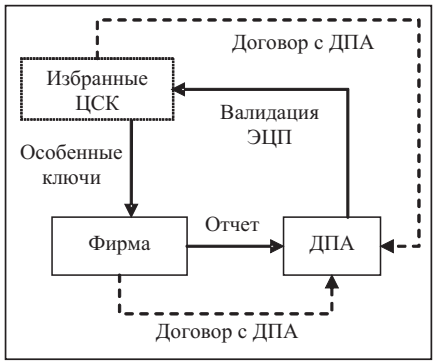

Рис. 7. Реальная схема сдачи отчетности в ДПА

В стандарте [5] определен набор свойств подписи, которые можно скомбинировать для получения форм ЭЦП, обеспечивающих выполнение разных требований. Указанные в нормативной части [5] поля содержат минимальный необходимый объем информации для обработки XML-документов. Результирующая XML-подпись отчета приведена на рис. 8. В формате подписи есть все необходимые поля для указания политики подписания, контрподписей (заверение директором подписи бухгалтера), временных штемпелей, сертификатов атрибутов, сертификатов органов штемпелевания времени, сертификатов открытых ключей и т.п. Отметим, что механизм сертификатов атрибутов более гибок для сертификации ролей субъектов в сценариях, описанных в политике подписания.

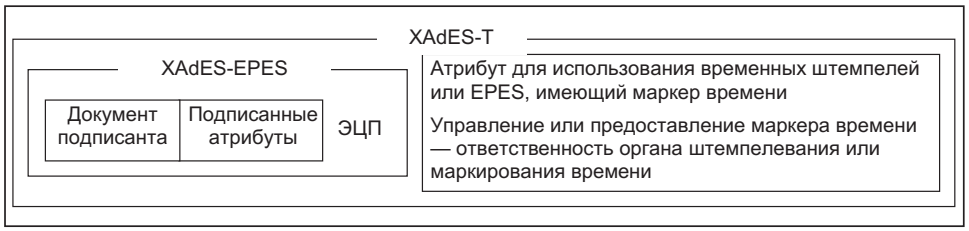

Рис. 8. XML-подпись отчета

Штемпелевание времени. В Украине отсутствует технологическая и организационная база поддержки временных штемпелей, хотя существует законодательная база, регламентирующая даже нотариально заверенные ЭЦП. Отсутствие временных штемпелей в ЭЦП и/или транспортируемом сообщении приводит к невозможности корректной обработки отчета, если он подписан в спорных ситуациях, например при компрометации сертификата открытого ключа и/или окончании срока приема отчета. Временные штемпели важны при валидации ЭЦП согласно политике подписания, например при регламентации времени наложения ЭЦП директором и бухгалтером.

Временные штемпели — это необходимый компонент для долгосрочного хранения квитанций о сдаче отчетов, необходимых при проверке ДПА своих клиентов, поскольку при компрометации одного из сертификатов в цепочке сертификации квитанция не может быть валидной, т.е. представленной как доказательство сдачи

отчета. В общем случае сроки подписания документов чрезвычайно важны для бизнеса и их невозможно гарантировать без указания надежного времени, которым являются временные штемпели.

Для решения поставленных задач необходимо создать органы штемпелевания времени, действующие согласно [3] и предоставляющие услуги согласно [4].

ЗАКЛЮЧЕНИЕ

Развитие Национальной системы ЭЦП имеет политический подтекст вследствие последней редакции Закона Украины № 852–15 [2], в которой контролирующий орган перебрал на себя больше полномочий, чем в предыдущей редакции этого Закона. С позиций системного анализа нарушена концепция распределения функций в инфраструктуре независимых оценщиков. Так, ЦЗО только аккредитует ЦСК, а техническим надзором за их деятельностью (качеством предоставляемых услуг) занимается контролирующий орган. Значит, он должен нести единоличную ответственность за все случаи компрометации ключей, хотя в новой редакции Закона эта функция осталась за ЦЗО. Вообще монополизация контролирующим органом сферы развития Национальной системы ЭЦП существенно тормозит ее развитие и всего информационного общества и, как следствие, не способствует конкурентоспособности Украины на мировом рынке.

Принятие Технического регламента, основанного на ДСТУ, гармонизированных с международными (в первую очередь, с европейскими) и де-факто стандартами (например, RFC), и поддержанного тестовым стендом валидации функций каждого ЦСК (при необходимости каждого владельца ЭЦП), является минимаксным способом достижения внутренней и внешней интероперабельности Национальной системы ЭЦП с возможностью кроссертификации с разными государствами. В настоящее время разработан достаточный набор национальных стандартов для инициализации процедуры создания Технического регламента.

СПИСОК ЛИТЕРАТУРЫ

1. ДСТУ ETSI TR 102 045 V1.1.1 (2003-03) Електронні підписи й інфраструктури (ESI). Політика підписів для розширеної бізнес-моделі.
2. Закон України від 22.05.2003 № 852-15 «Про електронний цифровий підпис».
3. ДСТУ ETSI TS 102 023 V1.2.1 (2003-01) Електронні підписи й інфраструктури (ESI). Вимоги політики для органів штемпелювання часу.
4. ДСТУ ETSI TS 101 861 V1.3.1 (2006-01) Профіль штемпелювання часу.
5. ДСТУ ETSI TS 101 903 V1.3.2 (2006-03) Розширені електронні XML-підписи (XAdES).
6. ДСТУ ETSI TS 101 733 V1.7.3 (2007-01) Електронні підписи й інфраструктури (ESI). CMS розширені електронні підписи (CAdES).
7. ДСТУ-П CWA 14172:2008 Настанова Європейської Ініціативи стандартизації електронних цифрових підписів з оцінювання відповідності (у восьми частинах).
8. ДСТУ ETSI TS 102 176-1 V2.0.0 (2007-11) Електронні підписи й інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Ч. 1. Геш-функції й асиметричні алгоритми.
9. Наказ ДПА України «Уніфікований формат транспортного повідомлення при інформаційній взаємодії платників податків і податкових органів в електронному вигляді телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису» від 22.07.2008 № 485.
10. RFC 821 Simple Mail Transfer Protocol.
11. Наказ ДПА України «Про подання електронної податкової звітності» від 10.04.2008 № 233.
12. Наказ ДПА України «Про затвердження формату (стандарту) електронного документа звітності платників податків» від 03.05.2006 № 242.
13. Закон України від 22.05.2003 № 851-15 «Про електронні документи та електронний документообіг».
14. IETF RFC 2459 Профіль сертифікатів й Інтернет-інфраструктури відкритих ключів X.509.

Поступила 08.07.2009