Об интероперабельности и безопасности Национальной системы электронных цифровых подписей в Украине. По сути вопроса

«Але сумна історія, що її мені розказала сердешна Тарасевичівна, повинна примусити і німого говорити, і глухого слухати.
… А я все ж волію додержувати стилю класичного;…»
Т.Г.Шевченко, «Музика (2)» (1855. 15. I. Новопетровський форт)

Мартыненко С.В, канд.физ.-мат.наук

Рассмотрено текущее состояние вопроса функциональной совместимости (интероперабельности) и безопасности Национальной системы электронных цифровых подписей в Украине, проблемы и пути их решения.

Как известно, в электронном мире, где все системы тесно взаимосвязаны и взаимозависимы, возможность взаимодействия между программными, программно-аппаратными продуктами разных производителей (интероперабельность) различных систем/подсистем приобретает особое значение. Это очень актуально для систем электронной отчетности (например, налоговая отчетность), электронного правительства, систем предоставления широкого спектра коммерческих электронных услуг и других электронных «массовых продуктов». Задачей эффективного электронного правительства является улучшение обслуживания граждан и процессов обмена информацией (общение) между правительственными структурами. Для достижения этой цели, электронное правительство требует механизмов взаимодействия, которые позволят ряду правительственных учреждений предлагать он-лайн доступ к своим услугам и принимать участие в процедурах услуг, которые предоставляются несколькими государственными учреждениями/ ведомствами (услуги «единого окна»).

Вопрос разработки открытых к взаимодействию продуктов Национальной системы электронных цифровых подписей (НСЭЦП) был и остается достаточно острой проблемой в Украине. Существует ряд публикаций на эту тему, где отдельные проблемы освещены правильно. Однако, из-за поверхностного уровня анализа и, возможно, непонимания авторами сути вопроса, в этих публикациях даются предложения, которые способны завести проблему в очередной глухой угол. Именно это и прислужило причиной написания этой публикации.

Начнем с согласования некоторых определений.

Интероперабельность, функциональная совместимость (Інтероперабельність, функціональна сумісність; interoperability, способность к совместной работе, *взаимодействию*) в общем понимании – это способность программных, программно-аппаратных продуктов разных производителей взаимодействовать и функционировать между собой.

В соответствии с Директивой Европейской комиссии [1], *интероперабельность* может быть определена как «*возможность обмена информацией и взаимного использования информации, которая получается в результате обмена*».

Более полное техническое определение можно найти в документе [2] европейской программы IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens – Интероперабельное предоставление услуг европейского электронного правительства государственным администрациям, бизнесу и гражданам): «*Интероперабельность – это способность систем информационных и коммуникационных технологий (ИКТ) и бизнес-процессов, которые они поддерживают, к*

обмену данными и к совместному (коллективному) использованию информации и знаний». Целями инфраструктуры (Framework) европейской интероперабельности является, в частности, поддержание стратегии ЕС относительно обеспечения электронных услуг, ориентированных на пользователя, путем взаимодействия служб и систем между государственными администрациями, а также между государственными администрациями и общественностью (гражданами и предприятиями) на общеевропейском уровне.

Следует рассматривать *три аспекта* интероперабельности [2]:

- *Организационная интероперабельность*. Этот аспект взаимодействия касается определения целей бизнеса, моделирования бизнес-процессов и обеспечения сотрудничества государственных администраций, которые хотят обмениваться информацией и имеют (могут иметь) различные внутренние структуры и процессы. Кроме того, организационная интероперабельность направлена на решение требований сообщества пользователей путем создания услуги, которая отвечает требованиям, и которая является легко идентифицируемой, доступной и ориентированной на пользователя.
- *Семантическая интероперабельность*. Этот аспект взаимодействия позволяет гарантировать, что точное значение информации, которой обменялись, будет понятным для любой другой прикладной программы (приложения), которая изначально не была разработана для этой цели. Семантическая совместимость позволяет системам объединить полученную информацию с другими информационными ресурсами и обрабатывать ее надлежащим образом.
- *Техническая интероперабельность*. Этот аспект взаимодействия охватывает технические вопросы, связанные с компьютерными системами и услугами. Он включает в себя основные аспекты, такие как открытые интерфейсы, службы взаимодействия (interconnection services), интеграцию данных и вспомогательное программное обеспечение (middleware), представление данных (data presentation) и обмен данными, доступность и безопасность услуг.

Таким образом, внедрение услуг электронного правительства на европейском уровне требует рассмотрения проблем взаимодействия с точки зрения *организационных, семантических и технических аспектов*.

В дополнение к общеевропейским стандартам и программам следует отметить, что существуют и соответствующие национальные программы/ стандарты, например, в Германии SAGA (Standards and Architectures for e-government Applications – Стандарты и архитектуры для приложений электронного правительства) [3] и др.

Не рассматривая в рамках данной публикации два первых из указанных аспектов, которые являются принципиально важными, сделаем лишь короткое замечание. На современном этапе отдельные рекомендации относительно и*нтероперабельности в* НСЭЦП Украины сводятся к внедрению некоего «универсального транспортного/ цифрового конверта», как панацеи для решения всех проблем. При этом «транспортный конверт» (например, как схема XML-документа) создается/ разрабатывается заново (для использования исключительно в Украине), не анализируя и не используя уже существующие международные/ европейские стандарты относительно таких систем обмена, и подается без какого-либо моделирования бизнеса-процесса, без создания основного и альтернативного потока документов (в терминах языка UML, см., например, стандарты S.W.I.F.T., ISO 20022, спецификации программы IDABC) и т.п. В результате обнаруживается отсутствие принципиально важных компонентов/ составляющих процессов, например, процедуры отзыва/ отмены ошибочно отправленного документа, не регламентированы действия во внештатных ситуациях и при возникновении ошибок на любом из этапов жизненного цикла и т.п..

Современной «модой» стало использование в качестве «транспортных конвертов» XML-документов. Но при этом, как правило, не предоставляются XML-схемы, не

определяется пространство имен, не используются стандарты (форматы) цифровой подписи и шифрования XML документов и т.п.. Примерами «транспортных конвертов» украинского производства являются, в частности, соответствующие конверты налоговой отчетности ГНА Украины (приказ от 11.02.2011 г. № 90), и в целом органов государственной власти (Приказ Министерства образования и науки, молодежи и спорта от 20.10.11 г. № 1207) и др. Но, если в спецификации XML-документа отсутствуют XSD-схема, и/или такие атрибуты как «пространство имен» (namespace, targetNamespace), «кодирование» (encoding) и некоторые другие, если в спецификации присутствуют «уникальные» идентификаторы (ID) без четкого определения правил формирования их значений (где их брать, кто их назначает …), то для интероперабельных систем эту спецификацию не следует даже читать, не говоря уже о ее реализации. Например, «пространство имен» (namespace) используется для локализации имен атрибутов в пределах схемы документа. Для интероперабельности мы ставим целью применения расширяемого языка разметки (XML), где один XML-документ может содержать элементы и атрибуты (называются «словарь разметки»), которые определены для использования несколькими модулями программного обеспечения. Одним из требований модульности при использовании словарей разметки является отсутствие проблем «распознавания» (recognize) и «столкновения/ коллизий» (collision). Т.е., программные модули должны быть способны распознать теги и атрибуты, которые необходимо обрабатывать, даже в условиях «столкновений», возникающих при разметке, предназначенной для другого пакета программного обеспечения, который использует тот же тип элемента или то же самое имя атрибута. Для невозможности проблем распознавания и коллизий и назначается «пространство имен» (namespace).

Вывод можно сделать сразу - внедрение подобного «транспортного конверта» не только не приблизит, а наоборот, навредит интероперабельности в НСЭЦП Украины. Не следует изобретать украинские «универсальные транспортные конверты» и протоколы, необходимо использовать соответствующие международные/ европейские стандарты (см. далее), которые уже прошли как теоретический анализ, так и практическую апробацию.

В заключении *организационной и семантической интероперабельности* следует также подчеркнуть, что и Национальный банк Украины не может быть в стороне от этого процесса. Так как ряд услуг электронного правительства может быть (либо уже является) платным, а также учитывая то, что применение финансовых инструментов требует таких систем, как электронная коммерция, электронная таможня, система контроля за возмещением НДС и т.п., НБУ также необходимо разработать соответствующие технические спецификации (перечень стандартов) и требования относительно интероперабельности. В основу спецификаций должны быть положены международные/ европейские стандарты, например, соответствующие спецификации программы IDABC и, конечно, ISO 20022.

Для дальнейшего рассмотрения проблем *Технической интероперабельности,* будем считать, что два первый из указанных выше аспектов интероперабельности соответствующим образом (профессионально) уже рассмотрены и решены. Итак, как указывалось выше, *Техническая интероперабельность* включает в себя [2]:

- открытые интерфейсы,
- службы межсистемной связи/ взаимодействия (interconnection services),
- интеграцию данных и вспомогательное программное обеспечение (middleware),
- представление данных (data presentation) и обмен данными,
- доступность,
- безопасность услуг в целом, и конфиденциальность персональных данных в частности.

Основными *принципами интероперабельности* являются (классически):

- Открытость интерфейсов,
- Следование стандартам,

- Транспортабельность данных.

Из составляющих технической интероперабельности здесь рассмотрим детально лишь следующие ключевые составляющие НСЭЦП:

а) *криптографические модули* – программные, программно-аппаратные средства криптографической защиты информации (КЗИ);

б) *форматы объектов системы цифровых подписей и шифрования* – форматы X. 509 сертификатов, цифровой подписи/ шифрования и других криптографических объектов НСЭЦП.

Открытость интерфейсов (первый принцип интероперабельности) означает, что средство КЗИ имеет открытый «Интерфейс прикладного программирования» (Application Programming Interface, API) – набор классов, процедур, функций, структур и констант, которые предоставляются средством КЗИ для использования во внешних программных продуктах. API используется для написания прикладных программ (приложений). Следует отметить, что термин «открытость» API означает, что интерфейс средства КЗИ отвечает определенным стандартам (принцип *следования стандартам*) для средств КЗИ.

Следование стандартам (второй принцип интероперабельности) – это, кроме стандартов API, также, и даже главным образом, следование стандартам безопасности для криптографических модулей. Такими общеизвестными и признанными стандартами является стандарт США «FIPS 140-2» [4] и международные стандарты серии «Общие критерии оценивания защищенности информационных технологий (Common Criteria for Information Technology Security Evaluation), или более короткое название «Общие критерии» (Common Criteria, CC) – ISO/IEC 15408-1: 2009 [5], ISO/IEC 15408-2:2008 [6], ISO/IEC 15408-3:2008 [7]. В рамках Европейского Союза дополнительно применяются стандарты ДСТУ CWA 14365-2:2009 [8], ДСТУ CWA 14167-3: 2008 [9], ДСТУ-П CWA 14172-5:2008 [10], ДСТУ-П CWA 14172-7:2008 [11], ДСТУ CWA 14355:2009 [12], CWA14169:2004 [13], CWA 14170:2004 [14].

Следует отметить, что интероперабельность и безопасность по сути являются антагонистическими понятиями - чем выше требования безопасности, тем, как правило, значительно тяжелее обеспечить интероперабельность, и наоборот. Для средств КЗИ нужно объединить интероперабельность и безопасность наиболее оптимальным образом, только в этом случае получим юридически значимый электронный документооборот.

Транспортабельность данных (третий принцип интероперабельности) относительно средств КЗИ означает, в частности, что при замене одного средства КЗИ другим обеспечивается возможность экспорта/импорта данных, которые хранятся в них, т.е. криптографических ключей, X. 509 сертификатов и т. д.

Интероперабельность НСЭЦП, в разрезе составляющих, которые здесь рассматриваются, по сути означает, что:

1) документы (данные), подписанные цифровой подписью и зашифрованные с помощью криптографического модуля одного производителя, могут быть расшифрованы и проверена подпись с использованием криптографического модуля другого производителя; аналогично и другие криптографические объекты, такие как X.509 сертификаты, списки отзыва (CRL), метки времени и т.д.;

2) прикладная система (приложение), разработанная для работы с криптографическим модулем одного производителя, не нуждается в доработках (модернизации, внесении изменений и т.д.) при переходе к/добавлении криптографического модуля другого производителя.

Рассмотрим ключевые проблемы (барьеры), текущее состояние интероперабельности и безопасности НСЭЦП Украины, отдельные публикации на эту тему и высказанные в них предложения (рекомендации).

Проблема №1. Несоответствие законодательства Украины законодательству ЕС

Базовым европейским законодательным актом является Директива 1999/93/ЕС [16], а в Украине соответственно Закон Украины «Об электронной цифровой подписи» [17].

Приведем сравнительную таблицу основных расхождений указанных законодательных актов по базовым терминам:

Закон Украины	Директива ЕС (официальный перевод)
електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;	*електронний підпис* – дані, поданні в електронній формі, які додаються або логічно об'єднуються з іншими електронними даними та які служать в якості метода засвідчення достовірності. *Комментарий. Это официальный перевод, но «метод засвидетельствования достоверности» в оригинале – это «method of authentication», что в информационных технологиях означает:* - *проверить целостность данных, и* - *идентифицировать подписанта данных.* *См., например, Barron's Banking Dictionary: «Authentication – Legal verification of the genuineness of a bond, document, or signature. In electronic funds transfers, authentication is a method of verifying that a payment instruction has in fact originated at the sending bank, and has not been tampered with by an unauthorized party» (Правовая проверка подлинности обязательства, документа или подписи. В электронном переводе средств, аутентификация - это метод проверки того, что платежное поручение, в сущности, возникло в банке-отправителе, и не было изменено посторонними лицами).*
електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його *цілісність* та *ідентифікувати* підписувача.	Термин отсутствует *Комментарий. По смыслу ЭЦП – это некоторая ограниченная электронная подпись Директивы ЕС. Ограничивается тем, что она получается в результате криптографического преобразования.*
Термин отсутствует *Комментарий. Совместимость ЭЦП с определением «усовершенствованная цифровая подпись» только по п.п. (b) и (d)*	***удосконалений електронний підпис*** означає електронний підпис, який відповідає наступним вимогам: (a) він пов'язаний винятково з особою, що підписалась; (b) він дає можливість ідентифікувати особу, що підписалась; (c) він створений за допомогою засобів, які особа,

Закон Украины	Директива ЕС (официальный перевод)
	що підписалась, може тримати під своїм повним контролем; і (d) він пов'язаний з даними, до яких він відноситься у такий спосіб, що будь-яку подальшу зміну даних можна виявити;
надійний засіб електронного цифрового підпису – засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. *Комментарий: Определение, приведенное в Законе Украины, не требует выполнения требований (a), (c) Директивы ЕС для усовершенствованной электронной подписи. Определение Закона разрешает произвольную трактовку «надежности» (в том числе, на уровне подзаконных актов).*	*безпечний механізм створення підпису* - означає механізм створення підпису, який відповідає вимогам, викладеним у Додатку III: a) дані, які використовуються для вироблення підпису, можуть виникнути на практиці лише один раз, а їх секретність забезпечується; b) дані, які використовуються для вироблення підпису, із значною долею впевненості не можуть вилучатися з цих механізмів, а підпис захищається від підробки за допомогою використання доступних технологій; c) дані, що створюють підпис, які використовуються для вироблення підпису, можуть бути надійно захищені законною особою, що підписалась від використання його іншими особами.
посилений сертифікат відкритого ключа (далі – посилений сертифікат ключа) – сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.	Термин отсутствует
Термин отсутствует	термін «*кваліфікований сертифікат*» (qualified certificate) означає сертифікат, який відповідає вимогам, викладеним у Додатку I (Вимоги до кваліфікованих сертифікатів), і видається постачальником послуг сертифікації, який виконує вимоги, викладені у Додатку II (Вимоги до постачальників послуг сертифікації, що видають кваліфіковані сертифікати);
Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо: електронний цифровий підпис *підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;*	Держави-члени забезпечують, щоб *удосконалені електронні підписи, засновані на кваліфікованих сертифікатах і створені за допомогою безпечних механізмів створення підпису*: a) задовольняли юридичним вимогам до підписів стосовно даних, поданих у електронній формі, так само, як підпис, написаний власноручно, задовольняє вимоги стосовно даних, нанесених на папір; і b) були прийнятними в якості доказів у судочинстві.

Итак, имеем следующее несоответствие юридической силы/ правового статуса:

Закон Украины	Директива ЕС
1. електронний цифровий підпис *підтверджено* з використанням 2. *посиленого* сертифіката ключа 3. за допомогою *надійних* засобів цифрового підпису;	1. *удосконалені* електронні підписи, 2. засновані на *кваліфікованих* сертифікатах і 3. *створені* за допомогою 4. *безпечних* механізмів створення підпису

Таким образом, имеем следующие основные несоответствия:

1) «посилений сертифікат» (усиленный сертификат) Закона Украины не соответствует «квалифицированному сертификату» Директивы ЕС,

2) «надійний засіб ЕЦП» (надежное средство ЭЦП) Закона Украины не соответствует «безопасному механизму создания подписи» Директивы ЕС.

3) По Закону Украины для обретения юридической силы подлежит контролю (и требуется безопасность) лишь этап проверки подписи («електронний цифровий підпис підтверджено з використанням …» - электронная цифровая подпись подтверждена с использованием …»), а Директива требует контроль на этапе создания («створені за допомогою …» - «созданные при помощи…»).

Итак, базовые термины Закона Украины не соответствуют терминам Директивы ЕС, нет общих/ совместимых критериев и соответствия относительно юридической силы/ правового статуса электронной (цифровой) подписи между Законом Украины и Директивой ЕС.

Наиболее критическим является значительно сниженный (законодательно) уровень безопасности ЭЦП Украины по сравнению с цифровой подписью ЕС, что отражается на других законодательных и нормативных актах.

Кстати, в России в свое время был принят аналогичный закон (от 08.11.2007 г., предыдущий в 2002), который имел такие же недостатки неурегулированности определений и терминов между законодательством РФ и ЕС. Эти недостатки были учтены и устранены в новой редакции Закона «Об электронной подписи» 2010 года, где определено три вида электронной подписи - *простая, усиленная и квалифицированная.*

Проблема №2. Низкий уровень стандартизации НСЭЦП. Тестирование соответствия в сфере КЗИ

Об экспертизе криптографических средств

Отсутствуют четкие технические требования (программы тестирования, тестовые вектора и т.п.), которым должны удовлетворять криптографические средства с целью получения сертификата соответствия или положительного экспертного заключения по результатам государственной экспертизы в сфере криптографической защиты информации (КЗИ). На текущий момент экспертиза осуществляется на соответствие техническому заданию производителя, которое предварительно подлежит согласованию с контролирующим органом в сфере КЗИ. Техническое задание - это «субъективный» документ (для одного и того же средства КЗИ может быть изложен на 20 или на 200 листах, в соответствии с требованиями международных стандартов или «на собственное усмотрение/ понимание»), а потому и положительное экспертное заключение является более «субъективным» документом, который не отражает действительного уровня соответствия, надежности и безопасности средства КЗИ.

Каждый лицензиат составляет и утверждает в контролирующем органе в сфере КЗИ собственную методику проверки правильности реализации или соответствия (тестирования). Такие методики также являются «субъективными», так как составляются «на собственное усмотрение/ понимание» лицензиата. Полнота и комплексность этих методик, как правило,

находится на неудовлетворительном уровне. Например, наиболее распространенная и наиболее, как считается, детальная методика тестирования правильности реализации ДСТУ 4145 содержит 266 тестовых векторов. Но в тестах «принимают участие» лишь три эллиптические кривые полиномиального базиса (173, 283, 431 бит) из 10-ти определенных стандартом и три эллиптические кривые оптимального нормального базиса (173, 233, 431 бит) из 5-ти определенных стандартом. Таким образом, любая ошибка в реализации (данных) других, не охваченных тестами и не проверенных, эллиптических кривых не может быть выявлена на этапе тестирования. В результате, если средство и имеет положительное экспертное заключение, то правильность его реализации, а соответственно, и интероперабельность, является сомнительной.

Хорошей государственной практикой является создание соответствующими государственными органами и открытое опубликование тестовых векторов и методик тестирования. Так, например, Национальный Институт Стандартов и Технологии США (NIST, National Institute of Standards and Technology) для нужд промышленности и пользователей в объективных, независимых тестах для информационных технологий, которые призваны помогать компаниям выпускать следующее поколение продуктов и услуг, разрабатывает серии криптографических тестов и тестов интероперабельности PKI (Public Key Interoperability), в частности, в рамках следующих программ:

- NIST программа валидации/ проверки правильности криптографических алгоритмов CAVP (Cryptographic Algorithm Validation Program) и
- NIST программа набора тестов интероперабельности открытых ключей PKITS (Public Key Interoperability Test Suite).

Разработанные тесты постоянно пересматриваются и обновляются с учетом приобретенного опыта при выявлении ошибок и несоответствий.

В качестве примера, можно обратиться к публикациям [20, 21] и др., а также к соответствующим сериям тестовых векторов, в частности:

- Алгоритма шифрования AES:
  - AES Known Answer Test (KAT) Vectors
  - AES Monte Carlo Test (MCT) Sample Vectors
  - AES Monte Carlo Test (MCT) Intermediate Values
  - AES Multiblock Message Test (MMT) Sample Vectors
- Алгоритма шифрования TDES:
  - Triple DES Known Answer Test (KAT) Vectors
  - Triple-DES Monte Carlo Test (MCT) Sample Vectors
  - Triple-DES Monte Carlo Test (MCT) Intermediate Values
  - Triple-DES Multiblock Message Test (MMT) Sample Vectors

Аналогично, существуют тестовые векторы для асимметрических алгоритмов RSA (ANSI X9.31), DSA (Digital Signature Algorithm), ECDSA (Elliptic Curve DSA; ANSI X9.62):

- 186-2 DSA Test Vectors
- 186-2 RSA Test Vectors
  - RSA SigVer PKCS1.5 Vulnerability Test Vectors
  - RSA SigVer X9.31 Vulnerability Test Vectors
- 186-2 ECDSA Test Vectors
- 186-3 DSA Test Vectors
- 186-3 RSA Test Vectors
- 186-3 ECDSA Test Vectors,

и генераторов случайных чисел, других криптографических алгоритмов и протоколов.

Назначение этих тестов состоит в предоставлении помощи компаниям при разработке интероперабельных совместных компонентов систем Инфраструктуры открытых ключей

(PKI), т.е. криптографических средств. Созданные наборы тестов позволят разработчикам и тестовым лабораториям определить соответствие программ/ продуктов PKI стандартам X.509. NIST открыто публикует информацию, необходимую для выполнения этих тестов (например, описание каждого теста, ожидаемые результаты теста, и любые сертификаты/ключи, списки отозванных сертификатов, необходимые для выполнения тестов и т.п.) в режиме он-лайн.

В Украине существуют определенные предложения/ публикации на эту тему, например, «Тестовый стенд для интероперабельности электронных цифровых подписей» [45] (Тестовый стенд). В публикации верно отмечено, что «*одна з основних причин нинішньої відсутності інтероперабельності Національної системи електронних цифрових підписів (НСЕЦП) – прогалини нормативної бази, що регулює технологічну та організаційну складові НСЕЦП*» (*«одна з основных причин нынешнего отсутствия интероперабельности Национальной системы электронных цифровых подписей (НСЕЦП) – пробелы нормативной базы, которая регулирует технологическую и организационную составляющие НСЕЦП*»). Для решения проблемы предлагается Тестовый стенд, в описании которого также верно отмечается, что создание тестовых стендов (добавим, и криптографических продуктов вообще) должно опираться *«… на принципи, обов'язкові відповідно до реалізації Загальних критеріїв IT-захисту [10], що пов'язано з необхідністю недопущення неякісних реалізацій і заснованих на них претензіях*» (*«… на принципы, обязательные в соответствии с реализацией Общих критериев IT-защиты [10], что связано с необходимостью недопущения некачественных реализаций и основанных на них претензиях*»). Но...

Но подобные предложения и соответствующие наборы тестов, как показано выше на примере NIST-тестов и соответствующих программ, - это задача, которая требует от разработчиков тестов высокой квалификации и профессионального уровня знаний по предмету тестирования. Во-вторых, Тестовый стенд, который предлагается использовать для тестирования соответствия, сам должен иметь сертификат соответствия (должен быть неким эталоном).

Относительно уровня квалификации Тестового стенда, который предлагается, то в нем имеем отождествление терминов «посилений» (усиленный) и «кваліфікований» (квалифицированный) сертификаты, о чем уже детально было сказано выше в Проблеме №1**.** Так, в описании Тестового стенда указано:
«*Загалом вимоги RFC 5280 профілює RFC 3739 (формально RFC 3280, але RFC 5280 замінив RFC 3280) на підтримку посилених сертифікатів. Вимоги RFC 3739 профілює ДСТУ ETSI TS 101 862 на підтримку посилених сертифікатів за визначеннями Директиви 1999/93/ЄС.*» (*В целом требования RFC 5280 профилирует RFC 3739 (формально RFC 3280, но RFC 5280 заменил RFC 3280) на поддержку усиленных сертификатов. Требования RFC 3739 профилирует ДСТУ ETSI TS 101 862 на поддержку усиленных сертификатов по определениям Директивы 1999/93/ЄС.)*
Но языком оригинала имеем «ETSI TS 101 862 V1.2.1 (2001-06) - Technical Specification. Qualified certificate profile». Итак, речь должна идти об «квалифицированном сертификате» ЕС, который не является эквивалентом «усиленного сертификата» Украины. Детальнее о качестве и уровне адаптации международных и европейских технических стандартов (ТК-20) рассмотрим далее.

Также, относительно уровня квалификации Тестового стенда, который предлагается, то в п. 2.3 «Пример реализации стенда» [45] указывается его состав, а именно: «*…використані бібліотеки для роботи з DER-закодованими ASN.1-нотаціями пакету Bouncy Castle, тестові сертифікати згенеровано в операційному середовищі FreeBSD 8.0 за допомогою утиліти OpenSSL*» («*…использованы библиотеки для работы с DER-кодированными ASN.1-нотациями пакета Bouncy Castle, тестовые сертификаты сгенерированы в операционной среде FreeBSD 8.0 при помощи утилиты OpenSSL*»). Указанные пакеты, Bouncy Castle и OpenSSL, – это

пакеты «свободного» программного обеспечения (с открытым кодом), которое (из текста лицензии): «*… предоставляется «как есть», без каких-либо гарантий, прямых или непрямых, включая, но не ограничивая гарантии пригодности для конкретных целей (товарного состояния, merchantability) …, не несет ответственности за какие-либо претензии, убытки или другие ответственности…*». К этому следует добавить, что версии указанных пакетов не определены, а это также является принципиальным моментом (например, у Bouncy Castle текущая версия 1.46, т.е. по меньшей мере, - это 46-я версия, без учета бета и промежуточных версий; с OpenSSL - аналогичная ситуация). Четко понятно, что такое «свободное» программное обеспечение не может быть «эталоном» для оценивания/ тестирования другого программного обеспечения (скорее может быть наоборот). Следует также отметить, что использование «свободного» программного обеспечения не является недопустимым, но обязательно требует дополнительного тестирования и проверки правильности, фиксации версии проверенного пакета, и только после этого может использоваться в безопасных системах.

Также, относительно уровня квалификации Тестового стенда, который предлагается, то в 2.2 сказано:
«*Приклад такої недобросовісної реалізації – просте вилучення всіх необхідних полів із сертифіката за допомогою стандартної/незалежної бібліотеки та наявності всіх полів, потрібних за нормативною базою. Цей підхід не проводить детального тестування, наприклад, в кореневому сертифікаті ЦЗО поле підпису, яке має ASN.1 тип BIT STRING згідно з RFC 5280, містить фактичний підпис, закодований як тип OCTET STRING (рис. 3). Верифікація підпису не буде успішною, зважаючи на два додаткових значення, що прикріплено до значення підпису та ідентифікують тип OCTET STRING і його довжину.*

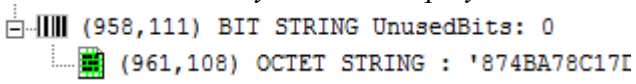


Рис. 3 Закодований підпис ЦЗО».

(«*Пример такой недобросовестной реализации – простое извлечение всех необходимых полей из сертификата при помощи стандартной/независимой библиотеки и наличия всех полей, необходимых по нормативной базе. Этот подход не проводит детального тестирования, например, в корневом сертификате ЦУО поле подписи, которое имеет ASN.1 тип BIT STRING согласно RFC 5280, содержит фактическую подпись, закодированную как тип OCTET STRING (рис. 3). Верификация подписи не буде успешной, учитывая два дополнительных значения, которые прикреплены к значению подписи и идентифицируют тип OCTET STRING и его длину.*

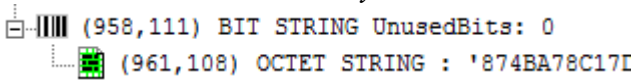


Рис. 3 Закодированная подпись ЦУО».)

Для объяснения сути «профессиональности» указанного утверждения (*недобросовестной реализации*) относительно подписи ЦУО следует предоставить следующую учебную информацию:

Стандарт RFC 5280:2008 [22] действительно определяет, что значение подписи кодируется как BIT STRING. Но здесь же в стандарте сказано, что «*детали этого процесса/ операции/ обработки определяются для каждого из алгоритмов …*» («*The details of this process are specified for each of the algorithms …*»)... Итак, не существует единого представления содержания BIT STRING для всех алгоритмов.

Стандарт RFC 3279:2002 [23] определяет значение подписи для алгоритма **DSA** (п. 2.2. 2) так:

При формировании подписи алгоритм DSA генерирует два значения. Эти значения обычно обозначают как r и s. Чтобы легко передать (transfer) эти два значения, как одну подпись, они должны быть ASN.1 закодированы, используя такую ASN.1 структуру:

```
Dss-Sig-Value  ::=  SEQUENCE  {
        r       INTEGER,
        s       INTEGER  }
```

Стандарт RFC 3279:2002 [23] также определяет значение подписи для алгоритма **ECDSA** (п. 2.2. 3) так:

При формировании подписи алгоритм ECDSA генерирует два значения. Эти значения обычно обозначают как r и s. Чтобы легко передать (transfer) эти два значения, как одну подпись, они должны быть ASN.1 закодированы, используя такую ASN.1 структуру:

```
Ecdsa-Sig-Value  ::=  SEQUENCE  {
      r    INTEGER,
      s    INTEGER  }
```

Спецификация «НАЦИОНАЛЬНАЯ СИСТЕМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ. Технические спецификации форматов представления базовых объектов» определяет значение подписи алгоритма **ДСТУ 4145-2002** (п. 1.3.11.6) как:

Электронная цифровая подпись ДСТУ 4145-2002 – это строка/последовательность октетов OCTET STRING (инкапсулировано в поле "signatureValue").

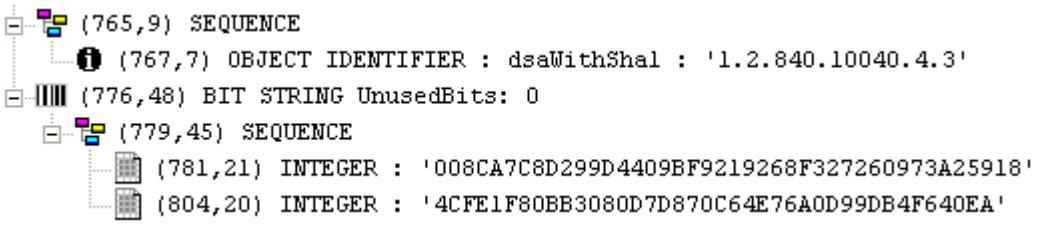
Спецификация «НАЦИОНАЛЬНАЯ СИСТЕМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ. Технические спецификации форматов представления базовых объектов» определяет значение подписи для алгоритма **ГОСТ 34.310-95** (п. 1.3.11.10) как:

Электронная цифровая подпись ГОСТ 34.310-95 – это строка октетов OCTET STRING (инкапсулировано в поле "signatureValue"):

```
SEQUENCE {
r INTEGER,
s INTEGER
}.
```

Таким образом, кроме алгоритма RSA, для которого значения подписи есть «чистой» строкой *BIT STRING*, все другие алгоритмы кодируют значение подписи или как *SEQUENCE*, *или как OCTET STRING или иначе, как это предусмотрено алгоритмом.*

Если же приведенных аргументов по этому вопросу (*недобросовестной реализации*) недостаточно для убедительности, то предлагаем обратиться к указанным выше тестовым векторам **NIST** программы PKITS (Public Key Interoperability Test Suite), где в частности содержится следующий тестовый сертификат (ValidDSASignaturesTest4EE.crt):

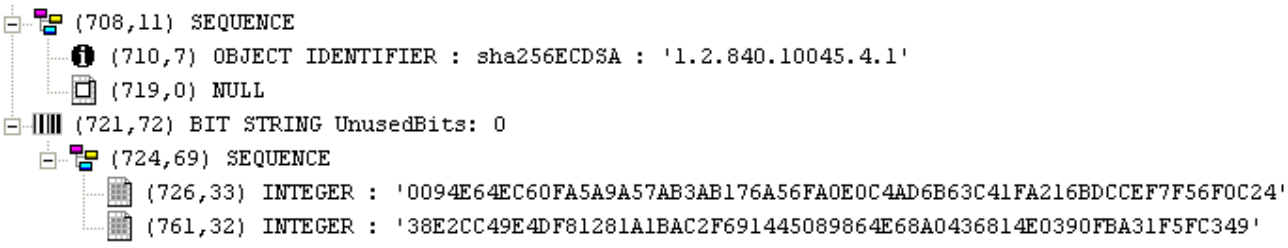


Если же приведенных аргументов по этому вопросу (*недобросовестной реализации*) недостаточно для убедительности, то предлагаем также обратиться к сертификату системы электронных паспортов **Германии**:

Издатель сертификата: CN = csca-germany, SERIALNUMBER = 001, OU = bsi, O = bund, C = DE

Владелец сертификата: CN = DS, SERIALNUMBER = 027, O = Bundesdruckerei Gmb, C = DE

Значение подписи:

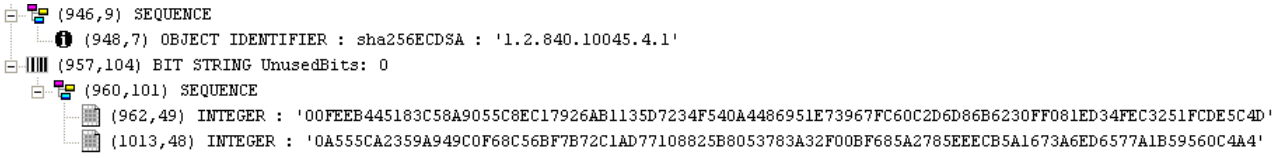


Если же приведенных аргументов по этому вопросу (*недобросовестной реализации*) недостаточно для убедительности, то предлагаем также обратиться к корневому сертификату системы электронных паспортов **Швейцарии**:

Издатель сертификата: CN = csca-switzerland-1, OU = Certification Authorities, OU = Services, O = Admin, C = CH

Владелец сертификата: CN = csca-switzerland-1, OU = Certification Authorities, OU = Services, O = Admin, C = CH

Значение подписи:



Вывод: Тестовый стенд, как представляется, не способен выполнять функции тестирования соответствия.

Проблема №3. Низкий уровень стандартизации НСЭЦП. Технические спецификации и адаптированные ДСТУ

Одной из проблем НСЭЦП является недостаточный уровень стандартизации в сфере криптографической защиты информации (КЗИ).

Существуют следующие возможности относительно повышения уровня стандартизации:

1. Адаптация (перевод на государственный язык) международных и европейских стандартов.
2. Принятие международных и европейских стандартов «методом обложки» (переводится название, титульный лист, и регистрируется как стандарт ДСТУ; содержание стандарта не переводится, а остается на языке оригинала).
3. Разработка и утверждение Технических спецификаций.

Разработка и утверждение Технических спецификаций не гарантирует отсутствия ошибок и недостатков, но срок их разработки и утверждения (приказом ответственного государственного органа/ учреждения) составляет несколько месяцев, что позволяет оперативно управлять данным процессом.

Принятие международных и европейских стандартов «методом обложки» считается хорошей практикой, так как является наиболее оперативной мерой. Но следует отметить, что такой подход имеет недостаток «неполного понимания», т.е. один и тот же текст на английском языке может по-разному восприниматься разными людьми. Этот недостаток может быть устранен путем выпуска словарей терминов, а при необходимости, уточнений/ рекомендаций на уровне Технических спецификаций.

Адаптация (перевод на государственный язык) международных и европейских технических стандартов имеет два существенных недостатка:

- Сроки адаптации составляют от 2- х (наиболее оптимистическая оценка) до 5-ти лет.
- Перевод часто выполняется непрофессионально, а потому пользоваться им невозможно, профессиональные пользователи обращаются к оригиналу.

Для доказательства приведем некоторые примеры непрофессиональности адаптации. Следует подчеркнуть, что примеры даются, основываясь как на проектах адаптированных стандартов, так и на уже действующих. На проекты в свое время были представлены замечания и предложения относительно внесения изменений, но ряд наиболее принципиальных замечаний был все же отклонен ТК-20. Теперь, если откровенно, покупать адаптации такого качества не представляется целесообразным, поэтому в работе лучше пользоваться оригиналами.

О непрофессиональности перевода (на примерах)

Рассматриваются примеры из ряда стандартов ДСТУ ETSI и ДСТУ CWA. Технический комитет, ответственный за этот стандарт – это ТК-20 «Информационные технологии».

1) Относительно терминов «посилений» (усиленный) и «кваліфікований» (квалифицированный)

Об отличии указанных терминов на законодательном уровне сказано выше при рассмотрении Проблемы №1 (Несоответствие законодательства Украины законодательству ЕС).

В ДСТУ ETSI TS 102 176-1 [24] раздел «Национальное вступление» имеем:

«У CWA 14167-1:2004 уведено термін «кваліфікований підпис», визначений у Директиві ЄС як розширений електронний підпис (advanced electronic signature), заснований на посилених сертифікатах (qualified certificate), створених безпечними (надійними) засобами накладання електронних підписів (secure signature creation device). Згідно з Законом України «Про електронний цифровий підпис» від 22 травня 2003 р. №852-IV вважають юридично правомочним (валідним) термін «кваліфікований підпис». »

Таким образом, имеем два разных перевода одного термина *qualified:*

qualified certificate - посилений сертифікат (усиленный сертификат);

qualified signature - кваліфікований підпис (квалифицированная подпись).

Англо-украинские словари предоставляют следующие переводы «*qualified*»: *компетентный, сведущий, подходящий или правомочный*. Ни один из возможных переводов не указывает на то, что можно перевести это слово как *«усиленный».*

В ДСТУ ETSI TS 102 045:2009 [25], в разделе раздел «Национальное вступление» имеем аналогичное, а также по тексту:

ДСТУ ETSI	ETSI
Директива 1999/93/ЕС [5] передбачає еквівалентність рукописних підписів, коли	Directive 1999/93/EC [5] provides for the equivalence to handwritten signatures where an

ДСТУ ETSI	ETSI
електронний підпис підтримано посиленими технічними засобами безпеки (стаття 5.1).	electronic signature is supported by enhanced technical security measures (article 5.1).
[9] ETSI TS 101 862 Профіль посиленого сертифіката	[9] ETSI TS 101 862 Qualified Certificate profile
посиленому сертифікаті й згенерованим безпечним засобом створення підпису, зазвичай називають “кваліфікованим електронним підписом”. Як визначено в додатку I, посилений сертифікат має випускати Орган сертифікації, що виконує вимоги Додатку II.	qualified certificate and created on a secure signature creation device, usually known as a "qualified electronic signature." A qualified certificate, as defined in annex I must be issued by a Certificate Authority complying with annex II.

Перечень примеров можно продолжать и продолжать… Это имеет место почти во всех стандартах серий ДСТУ ETSI и ДСТУ CWA Технического комитета ТК-20.

Как видно из приведенных примеров, идет выборочная (сознательная!?) подмена термина «квалифицированный» на термин «усиленный». Учитывая принципиальное отличие указанных терминов на законодательном уровне (см. выше Проблему №1), можно, как представляется, сделать вывод, что перевод не отвечает содержанию оригинала стандартов, т.е. не является идентичным.

2) Относительно перевода модальных глаголов для обозначения уровня требований

Уровень требований стандартов играет ключевую роль в технических стандартах, так как определяет обязательность или не обязательность (опциональность) реализации определенных особенностей/ атрибутов и т.п., рекомендуется или не рекомендуется (хотя не запрещается) реализовывать, запрещается или нет и т.п.. Без четких определений уровня требований стандартов не может быть и речи об интероперабельности, так как каждый на свое усмотрение будет реализовывать то или иное подмножество свойств/ атрибутов/ алгоритмов, запрещать или разрешать и т.п..

Для определения уровня требований стандартов устоявшейся практикой является применение ключевых слов и толкование модальных глаголов для обозначения уровня требований в соответствии со стандартами RFC, как определено в RFC 2119 [34].

Речь идет о таких ключевых словах (словоформах) стандартов: "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", "OPTIONAL".

Приведем авторский перевод основного содержания RFC 2119 [34]:

1. MUST - Это слово, а также термины REQUIRED и SHALL используется для требований, которые являются абсолютно необходимыми в данной спецификации.

2. MUST NOT - Эта фраза или слова SHALL NOT обозначают абсолютный запрет в рамках спецификации.

3. SHOULD - Это слово, а также глагол RECOMMENDED используется для обозначения требований, от выполнения которых можно отказаться при наличии разумных причин. Однако в случае такого отказа следует помнить о возможных проблемах в результате отказа и принимать взвешенное решение.

4. SHOULD NOT - Эта фраза и глагол NOT RECOMMENDED используются относительно особенностей или функций, которые допустимы и могут быть полезными, но могут вызвать проблемы. При реализации таких опций следует учитывать возможность возникновения проблем и принимать взвешенное решение.

5. MAY - Это слово, а также прилагательное OPTIONAL обозначают элементы, реализация которых является необязательной. Одни разработчики могут включать данные опции в свою продукцию для расширения возможностей, а другие опускать с целью упрощения. Реализация, которая не включает ту или другую опцию, должна быть готова к работе с реализациями, которые используют эту опцию (возможно совместная работа будет обеспечиваться за счет некоторого уменьшения функциональности). Те, кто включает опцию реализации, должны быть готовы (естественно, без использования такой опции) к взаимодействию с реализациями, которые такую опцию не поддерживают.

6. Рекомендации по использованию. Приведенные в этом документе определения следует использовать очень осторожно. В частности, необходимо применять их лишь там, где это действительно продиктовано требованиями интероперабельности или для предотвращения ситуаций, когда может быть причинен вред (например, для ограничения чрезмерных повторов передачи). Например, такие обозначения недопустимо использовать для обозначения/ трактования преимуществ одной реализации по сравнению с другой, если это не продиктовано соображениями интероперабельности.

7. Вопрос безопасности. Рассмотренные здесь термины часто используются при обсуждении вопросов безопасности. Отказ от выполнения необходимых (MUST) или рекомендованных (SHOULD) требований или реализация недопустимых (MUST NOT)/ не рекомендованных (SHOULD NOT) может существенным образом влиять на безопасность. Авторы документов должны уделить внимание вопросам безопасности, чтобы не появлялись реализации с невыполненными требованиями или рекомендациями.

Представляется, что необходимо использовать следующие переводы указанных ключевых слов:

MUST, REQUIRED, SHALL – Необхідно/ Вимагається/ Повинні (Необходимо/ Требуется/ Должны),

MUST NOT, SHALL NOT – Неприпустимо/ Забороняється - Недопустимо/ Запрещается,

SHOULD, RECOMMENDED - Рекомендується/ Слідує - Рекомендуется/ Следует;

SHOULD NOT, NOT RECOMMENDED – Не рекомендується/ Не слідує - Не рекомендуется/ Не следует;

MAY, OPTIONAL – Можливо/ Опціонально/ Не обов’язково/ Додатково - Возможно/ Опционально/ Не обязательно/ Дополнительно.

Как известно, перевод модальных глаголов вызывает ряд трудностей [42], и потому одной из главных задач при адаптации (переводе) технических стандартов является максимально четко, без каких-либо возможностей неоднозначного толкования, определить требования, особенно требования безопасности.

С точки зрения пользователя адаптированных стандартов, и с целью максимальной минимизации возможных неоднозначных толкований требований обязательности, следует и даже необходимо использовать один и тот же термин (словоформу) не только в рамках одного отдельного стандарта, но и в рамках всей серии стандартов определенного раздела, например, «Информационные технологии». Так, из возможных вариантов перевода «Необхідно/ Вимагається/ Повинні - Необходимо/ Требуется/ Должны» следует, как представляется, использовать лишь один, например, «Повинні» («Должны»). **Главным фактором для технических стандартов есть не столько литературность перевода, сколько четкость и однозначность толкования требований.**

Учитывая вышесказанное, приведем для сравнения текст оригинала и перевода из CWA 14167-1:2003 [38]:

Оригинал	Перевод
All security requirements of this CWA are clearly stated and may be: • mandatory (indicated by MUST (NOT) or SHALL (NOT)); • optional (indicated by SHOULD (NOT) or (NOT) RECOMMENDED); • · permitted (MAY or MAY (NOT)).	Усі вимоги безпеки цього стандарту точно заявлено й можуть бути: • обов'язковими (позначено (НЕ) МАЄ або (НЕ) БУДЕ); • опціональними (позначено (НЕ) МАЄ або (НЕ) РЕКОМЕНДОВАНО); • - дозволеними (МОЖЕ або (НЕ) МОЖЕ).

Для того, чтобы понять проблему, заложенную таким переводом, достаточно обратиться к словарю украинского языка, например, «Академический толковый словарь (1970—1980)», и ознакомиться с толкованием «МАТИ» (http://sum.in.ua/s/maty) и «БУТИ» (http://sum.in.ua/s/buty), и сделать вывод о том, можно ли их толковать однозначно, а соответственно и реализовывать для интероперабельности решений.

Как следует из словаря, глагол «БУТИ» ни коим образом не употребляется для определения требований обязательности (а как будущее время, существование и др.). Глагол «МАТИ» в первую очередь ассоциируется для определения того, что кому-либо принадлежит что-либо, является его собственностью; владеть чем-то, занимать что-то и так далее – 5 первых толкований не имеют отношения к обязательности. И лишь на шестом месте мы находим: «6. з інфін. Вживається на означення того, що «*а) (що) повинно щось відбутися, настати. б) (хто) хтось повинен прийти, прибути куди-небудь чи бути присутнім десь. в) (що) повинно щось міститися де-небудь.*», причем подчеркнем - «с инф.», а толкование объясняется с помощью глагола «повинен» («должен»). Итак, как самостоятельный глагол «БУТИ», в соответствии с «Академическим толковым словарем (1970-1980)», не может никаким образом отвечать требованию обязательности, а глагол «МАТИ с инф.» с шестой попытки будет иметь верное толкование, как «повинен» («должен»).

Аналогично имеем и в ДСТУ ETSI TS 102 176-1 [24]:

Оригинал	Перевод
RFC documents use the terms SHALL, SHOULD, MAY, RECOMMENDED in order to allow for interoperability. The same terminology is used in the present document (see RFC 2119 [25]).	У документах RFC вжито терміни БУДЕ, МАЄ БУТИ, МОЖЕ, РЕКОМЕНДОВАНО для досягнення інтероперабельності. Цю термінологію вжито в цьому стандарті (див. RFC 2119 [25]).

Здесь дополнительно еще имеем следующее «предложение» ТК-20:

SHOULD- (Рекомендуется) = МАЄ БУТИ. (Рекомендуется?) = ДОЛЖЕН БЫТЬ.

Технические специалисты при изучении ДСТУ ETSI TS 102 176-1, с целью установления требований обязательности словоформы МАЄ БУТИ, как и в предыдущем случае, обращаются к словарю украинского языка, например, «Академический толковый словарь (1970—1980)», но «МАЄ БУТИ» можно найти лишь в разделе «БУТИ» (http://sum.in.ua/s/buty), о чем говорилось выше, хотя толкование словаря (*повинно щось відбутися, настати ...)* совсем не отвечает требованию стандарта «Рекомендуется».

Правилом перевода стандартов должно быть следующее: употреблять только те термины и словоформы, в которых толковый словарь приводит на ПЕРВОМ месте верное (с точки зрения контекста стандарта) толкование.

Можно с уверенностью утверждать, что почти никто из технических специалистов, для кого и предназначается перевод стандарта, не свяжет МАЄ или БУДЕ с обязательностью как

абсолютно необходимым требованием. Большинство технических специалистов свяжет МАЄ БУТИ как обязательное требование (должен), а не рекомендованное.

Если же в стандарте ключевые слова требований обязательности не пишутся большими буквами, то получаем «свободный» перевод, который вообще выходит за границы понимания требований обязательности (ДСТУ CWA 14167-2 [39]):

Перевод	Оригинал	Примечание
FAU_STG.2.3/TOE TSF гарантує, що [призначення: метрика для збереження контрольних звітів] контрольні звіти **буде** підтримано, якщо виконано умови: вичерпання сховища аудиту	FAU_STG.2.3/TOE The TSF **shall** ensure that [assignment: metric for saving audit records] audit records **will be** maintained when the following conditions occur: audit storage exhaustion.	Требование обязательности (**shall**) не учтено. «**буде**» используется для обозначения будущего времени, а не требования «рекомендовано» как в примерах выше
ATE_FUN.1.2C Плани тестів ідентифікують функції безпеки, які **буде** протестовано, (підлягають тестуванню) і описують мету тестів, які **буде** виконано (підлягають виконанню).	ATE_FUN.1.2C The test plans **shall** identify the security functions **to be** tested and describe the goal of the tests **to be** performed.	Требование обязательности (**shall**) не учтено вообще. «**буде**» использовано для обозначения будущего времени, а не требования «рекомендовано» как в примерах выше

На замечание по этому поводу, предоставленные в ТК-20 через НБУ, был получен категоричный отказ следующего содержания: «*Насамперед згадаємо, що неживі сутності нікому нічого не винні/повинні/зобов'язані. Тому слід вживати лише дієслово МАЄ….*». Оставим проблему перевода и применения модальных глаголов обязательности профессионалам, специалистам по лингвистической теории.

Но обратиться к украинской классике делу не повредит:

Название произведения Т.Г. Шевченко	**Цитата**
«Близнята (1)»	Та проте ці дрібнички спостеріг Степан Мартинович і казав якось у пасіці після читання Тита Лівія, що це недобре: однієї, мовляв, матері діти, то й усе **повинно** бути рівне.
«Близнята (2)»	Це слово мене здивувало: як! у цій мертвій пустелі дерево? І справді вже, якщо воно є, то **повинно** бути святе!
«Мандрівка з приємністю та й не без моралі (1)»	А по правді не **повинно** б так бути. Освіта **повинна** збагачувати, а не обкрадати людське серце.
«Мандрівка з приємністю та й не без моралі (1)»	За півгодини лекція готова, і згідно з умовою інструмент **повинен** бути відчинений.
«Музика (2)» (1855. 15. І. Новопетровський форт)	Але сумна історія, що її мені розказала сердешна Тарасевичівна, **повинна** примусити і німого говорити, і глухого слухати. …

Название произведения Т.Г. Шевченко	Цитата
	На мою думку, твори суто мистецькі не **повинні** описувати картин брудних, хоч це, нажаль, і ввійшло тепер у моду.
«Художник»	— Хто вам підказав, що в мене є його праця? — **Повинна** бути, — сказав він рішуче.
"Щоденник (1857-06)"	Правда — стара, отже **повинна** бути ясна, зрозуміла;
"Щоденник (1857-07)"	8 [липня]. Сьогодні відійшов поштовий човен до Ґурєва. Вітер зюд-вест. У середу або в четвер він **повинен** бути на Стрілецькій Косі, в 15 верствах від Ґурєва.
"Щоденник (1857-08)"	8 [серпня]. На людину, що ниділа, як я, сім літ у голій пустині, кожне, навіть богоспасаєме місто Бєлєбєй (найнікчемніше містечко оренбурзької ґубернії), **повинно** було б зробити приємне враження.
"Щоденник (1857-12)"	Портрет **повинен** бути схожий, бо не подібний до рисунків такого роду.

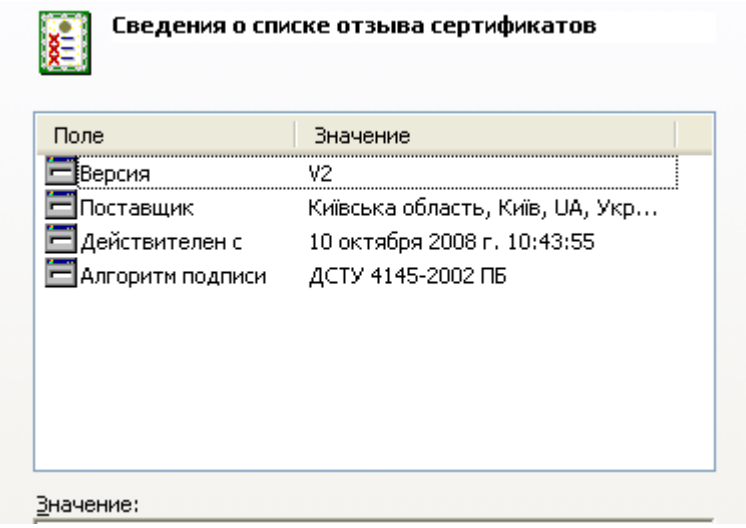
Таким образом, следуя Кобзарю, ***глагол*** *повинен/повинна/повинні (должен/должна/должны)* может применяться и относительно неживых сущностей. И потому «*…я все ж волію додержувати стилю класичного*» (Т.Г.Шевченко, «Музика (2)).

Категорический отказ со стороны ТК-20 относительно употребления глагола «повинні» («должны») тем более удивляет потому, что ряд стандартов, адаптированных именно самим ТК-20, употребляют глагол «повинні» («должны») для перевода MUST, REQUIRED, SHALL:

Стандарт	Цитата
ISO/lEC14888-1:2002 [36]	7.1. Щоб використати специфічний механізм підписування, потрібна специфічна геш-функція. Процес перевіряння **повинен** використовувати тільки цю специфічну геш-функцію.
ISO/lEC14888-1:2002 [36]	9. … Детерміноване свідоцтво **не повинне** передаватися перевірювачу, який також може його обчислювати …
ISO/lEC14888-1:2002 [36]	9.2 … Процес готування повідомлення **повинен** задовольняти одну з двох умов: - Повне повідомлення М **повинне** бути відновлюване для даних М1 і М2;
ДСТУ ISO/IEC 10118-2:2003 [37]	9.2 Вибирання параметрів Параметри L1, L2, та LH геш-функції, наведеної у даному розділі, **повинні** задовольняти: L1 = 3n, L2 = 9n, LH дорівнює 3n.
ДСТУ ISO/IEC 10118-2:2003 [37]	А.6 Мотивування … Ці значення **повинні** мати такі властивості:

Как видно из приведенных примеров, никаких сомнений относительно двойного толкования требований не может возникнуть - все требования четкие и однозначные.

Последствия несоблюдения (из-за неправильного толкования или др.) требований обязательности можно показать на примере списков блокированных сертификатов (CRL), которые формировались предыдущей версией ЦУО:



Как видно, CRL имеет версию 2, поле nextUpdate (следующее обновление) отсутствует.

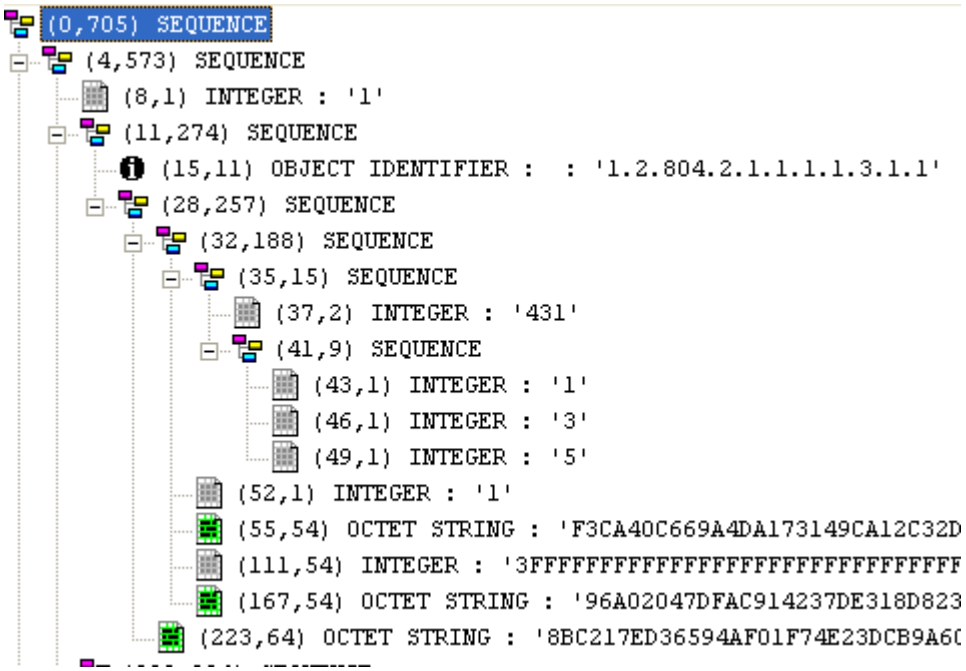
В соответствии со стандартом RFC 5280:2008 [22] (п. 5.1.2.5. Next Update) имеем следующее требование:

Оригинал	Перевод (авторский)
Conforming CRL issuers **MUST** include the nextUpdate field in all CRLs. Note that the ASN.1 syntax of TBSCertList describes this field as **OPTIONAL**, which is consistent with the ASN.1 structure defined in [X.509]. The behavior of clients processing CRLs that **omit** nextUpdate is not specified by this profile.	Эмитенты CRL, которые подчиняются правилам, **должны** включать nextUpdate поле во всех списках отозванных сертификатов. Обратите внимание, что ASN.1 синтаксис TBSCertList описывает поле як **ОПЦІОНАЛЬНОЕ**, что согласуется с ASN.1структурою, определенной в [X.509]. Поведение клиентов обработки списка отозванных сертификатов, которые **опускают** nextUpdate, не предусмотрена этим профилем.

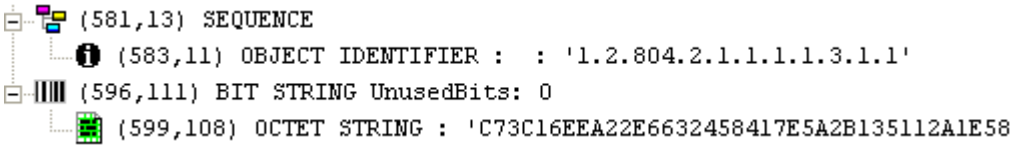
Итак, стандарт требует в качестве обязательного условия наличие поля nextUpdate, иначе стандарт не предусматривает/ не определяет «*поведение клиентов обработки*». Т.е. не существует единых правил обработки, а потому, не может быть и интероперабельности.

Второй пример с теми же списками блокированных сертификатов (CRL), которые формировались предыдущей версией ЦУО:

Структура TBSCertList (п. 5.1. CRL Fields стандарта), значение поля signature как AlgorithmIdentifier:



Структура CertificateList (п. 5.1. CRL Fields стандарта), значение поля signatureAlgorithm как AlgorithmIdentifier:



Очевидно, что поле signature не эквивалентно полю signatureAlgorithm (эквивалентность байт-к-байту).

В соответствии со стандартом RFC 5280:2008 [22] (п. 5.1.2.5. Next Update) имеем следующее требование:

Оригинал	**Перевод (авторский)**
5.1.1.2. signatureAlgorithm This field **MUST** contain the same algorithm identifier as the signature field in the sequence tbsCertList (Section 5.1.2.2).	5.1.1.2. signatureAlgorithm Это поле **должно** содержать тот же идентификатор алгоритму, что и поле signature в последовательности tbsCertList (п.5.1.2.2).
5.1.2.2. Signature This field **MUST** contain the same algorithm identifier as the signatureAlgorithm field in the sequence CertificateList (Section 5.1.1.2).	5.1.2.2. Signature Это поле **должно** содержать тот же идентификатор алгоритма, что и поле signatureAlgorithm в последовательности CertificateList (п.5.1.1.2).

Указанное требование является обязательным и означает, что поля signature и signatureAlgorithm, как AlgorithmIdentifier, должны (обязательно!) быть эквивалентными.

Из-за указанного несоответствия стандарту, обработка таких CRL списков ЦУО завершает с ошибкой (проверено для Microsoft Windows XP/2003/7/2008, Sun JRE 1.6, Oracle OAS и др.). Подчеркнем, причиной невозможности обработать CRL списки ЦУО предыдущей версии было не применение национального алгоритма подписи (ДСТУ 4145) для этих

списков, а именно несоответствие стандарту относительно обязательности требований эквивалентности полей signature и signatureAlgorithm.

Есть надежда, что эта проблема здесь освещена достаточно полно, чтобы понять ее сущность и пути решения. Следует лишь отметить, что переводы стандартов содержат, как представляется, также терминологические несоответствия относительно сугубо профессиональных терминов и значений информационных технологий, криптографии и защиты информации, но здесь этот вопрос не рассматривается.

Проблема №4. Низкий уровень академических работ и исследований в Украине

Об уровне научных фундаментальных исследований по вопросам, которые здесь рассматриваются, уже можно сделать вывод из предварительно рассмотренного уровня квалификации Тестового стенда (см. Проблему №2). К сожалению, ряд проектов типа *недобросовестной реализации* выполняется, как представляется, в бизнес-целях лицами, которые занимают государственные/ научные должности (админ. ресурс), что ухудшает перспективы интероперабельности.

В качестве примера, см. обращение к Директору Департамента информационно-аналитического обеспечения процессов налогообложения ГНА Украины (ttp://forum.sta.gov.ua/posts/list/34228.page), где указано, что:

«Інститут кібернетики як один із засновників Національної системи електронних цифрових підписів (НСЕЦП) виконав низку фундаментальних досліджень для вирішення проблем інтероперабельності (функціональної сумісності) об'єктів НСЕЦП щодо основних перешкод у розвитку електронної фіскальної звітності і електронного документообігу. Результати фундаментальних досліджень реалізовано у зареєстрованому центрі сертифікації ключів (ЦСК) «UPG-PKI» (http://ca.upg.kiev.ua/), який зараз проходить процедуру акредитації.»

Итак, можно толковать таким образом, что государственное научное учреждение, используя «*Результаты фундаментальных исследований»,* проведенных в нем за счет средств …(?), передало на основании …(?) эти результаты ООО «Юкрейн Проперти Групп» (http://upg.kiev.ua/) для внедрения в зарегистрированном центре сертификации для «решения» государственных проблем интероперабельности?...

О «фундаментальности» и уровне, основанном на пакетах «свободного» программного обеспечения, сказано выше на примере Тестового стенда.

Здесь отметим, что в письме в ГНА предлагаются следующие мероприятия (в кавычках приведены цитаты из письма от имени Института кибернетики/ ООО «UPG»):

3) Подписание электронных договоров между ГНА и субъектами предпринимательства:

«Підписування електронних договорів між ДПА і суб'єктами підприємництва з використанням зручних і звичних засобів MS Office та/або OpenOffice.»

4) Добавить к ДСТУ 4145 алгоритма подписи еще алгоритм RSA (комплект подписей SHA1withRSA):

«Міжнародний комплект підписів SHA1withRSA реалізовано у ПТК Центрального засвідчувального органу (позитивний експертний висновок 32206929.3КЦД.010.00.1).

Отже, в НСЕЦП можна застосувати міжнародні комплекти підписів, що значно спростить інтеграцію функцій ЕЦП у сторонні продукти здавання електронної фіскальної звітності, підтримку ЕЦП у шлюзі та внутрішньому електронному документообігу ДПА.»

5) К существующему шлюзу, который обрабатывает ДСТУ 4145, добавить еще один шлюз для международных ЭЦП:

«Застосування ДСТУ дозволить вилучити процедуру інтеграції модулів у шлюз, оскільки всі міжнародні ЕЦП, створені іншими криптомодулями, розшифровуватиме єдиний криптомодуль шлюзу. Причому розширення функцій шлюзу згідно з ДСТУ ніяк не вплине на функції обробки ЕЦП, заснованих на ДСТУ 4145.»

6) Применить международные стандарты XML-подписей:

«Щодо створення потенційної можливості функціонування кількох шлюзів передачі електронних звітів (див. п'яте питання) пропонуємо розпочати застосування міжнародних стандартів XML-підписів і розширюваної мови розмітки звітів XBRL як основного формату електронної фіскальної звітності. Цей формат застосовують у США і більшості країнах-членах ЄС як основний XML-базований формат здачі електронної фіскальної звітності. Застосування єдиного підходу XBRL до формування форм звітності із стандартними XML-підписами дозволить створити альтернативні шлюзи.»

Рассмотрим первый пункт: Подписание электронных договоров между ГНА и субъектами предпринимательской деятельности с использованием «*обычных средств MS Office и/или OpenOffice»*. Выше уже указывалось, что одной из решающих составляющих европейской программы IDABC интероперабельности электронного правительства [2] является безопасность услуг в целом, и конфиденциальность/ защита персональных данных в частности.

Коротко – в настоящий момент не существует международных/европейских стандартов относительно цифровой подписи/ шифрования документов MS Office (Word, Excel …). Существуют лишь международные и европейские стандарты для XML-документов и PDF-документов. Итак, «*использование удобных и обычных средств»* не всегда является приемлемым, если при этом совсем не рассматривается безопасность услуг в целом, и защита персональных данных в частности.

Рассмотрим второй пункт: Добавить комплект подписей SHA1withRSA.

Во-первых, замена одного криптографического алгоритма другим не может автоматически «*значно спростити інтеграцію функцій ЕЦП у продукти здавання електронної фіскальної звітності»*. Это зависит, как указано выше, от Организационной и Семантической интероперабельности, от верного решения *Технической интероперабельности,* что включает в себя [2], в частности:

- открытые интерфейсы,
- интеграцию данных и вспомогательное программное обеспечение (middleware),
- представление данных (data presentation) и обмен данными,
- безопасность услуг в целом, и конфиденциальность персональных данных в частности.

Более детально об истинных проблемах «*интеграции функций ЭЦП»* будет сказано далее. Если коротко, то замена одного комплекта подписи на другой не может обеспечить интероперабельность.

Во-вторых, комплект подписи SHA1withRSA с 01.01.2012 не рекомендован (из соображений безопасности) для использования [24].

Рассмотрим третий пункт: К существующему шлюзу, который обрабатывает ДСТУ 4145 добавить еще один для международных ЭЦП. При этом якобы «*всі міжнародні ЕЦП, створені іншими криптомодулями, розшифровуватиме єдиний криптомодуль шлюзу»*. Такая уверенность может быть только в случае незнания истинных причин несовместимости разных криптомодулей, которые рассматриваются далее в этой публикации (см. Проблему № 5 «Низкий уровень стандартизации НСЭЦП. Несовместимость разных криптомодулей»). Здесь лишь укажем, что переход на другие алгоритмы подписи, даже на международные,

автоматически не обеспечит совместимости криптографических модулей разных производителей, особенно это касается, к сожалению, украинских производителей.

Рассмотрим четвертый пункт: Применение международных стандартов XML-подписей. Такая позиция является верной, особенно потому, что ГНА использует документы формата XML. Но, следует отметить, что, с точки зрения реализации, XML-подпись и шифрование являются наиболее сложной задачей из такого ряда задач:

- подпись в формате PKCS#7/CMS (синтаксис криптографических сообщений);
- подпись PDF-документов;
- подпись XML-документов.

На сегодняшний день в Украине регламентировано (на уровне технических спецификаций) лишь подпись в формате PKCS#7/CMS (синтаксис криптографических сообщений), который и используется ГНА и другими участниками НСЭЦП, и который к тому же является простейшим с точки зрения реализации и интероперабельности.

Подпись PDF-документов стандартизируется международными и европейскими стандартами (в Украине не регламентирована). Реализация является более сложной задачей, так как требует: а) реализации подписи в формате PKCS#7/CMS, б) реализацию стандарта ISO 32000-1:2008 [26] с учетом серии стандартов ETSI TS 102 778 [27-33].

Подпись в формате XML также не регламентирована в Украине. Для обеспечения интероперабельности не помогут ни международные, ни европейские стандарты, так как они описывают универсальный формат с множеством вариантов и необязательных (опциональних) элементов/ компонентов подписи/ шифрования. Эти необязательные элементы по-разному (имеется в виду количество таких элементов) могут реализоваться разными разработчиками. Итак, без технической четкой регламентации формата XML подписи и шифрования его внедрение не поможет интероперабельности.

Таким образом, как представляется, приведенный пример не является образцом действительно научных фундаментальных исследований относительно НСЭЦП.

Проблема № 5. Низкий уровень стандартизации НСЭЦП. Несовместимость разных крипто модулей

Руководствуясь основными *принципами и*нтероперабельности (открытость интерфейсов, следование стандартам) [2], рассмотрим **главные причины** неинтероперабельности НСЭЦП, используя для примеров систему электронной отчетности ГНА Украины (аналогичное состояние дел и в других системах электронной отчетности, например, Пенсионном фонде Украины и др.):

1) «Многовекторность» технических спецификаций Украины

Под «многовекторностью» будем понимать несколько вариантов реализации, заложенные в технических спецификациях для одной задачи.

Так, в технической спецификации форматов объектов [40] фактически «удвоено» количество алгоритмов ДСТУ 4145-2002 - имеем не два алгоритма (полиномиальный базис и оптимальный нормальный базис), а фактически четыре:

Для формата Little-Endian (при определении параметров эллиптической кривой в сертификате):

полиномиальный базис 1.2.804.2.1.1.1.1.3.1.1

оптимальный нормальный базис 1.2.804.2.1.1.1.1.3.1.2

Для формата Big-Endian (при определении параметров эллиптической кривой в сертификате):

полиномиальный базис 1.2.804.2.1.1.1.1.3.1.1.1.1

оптимальный нормальный базис 1.2.804.2.1.1.1.1.3.1.2.1.1

Отличаются эти пары алгоритмов лишь форматом кодирования параметров точки эллиптической кривой в сертификате. Т.е. никакого выигрыша, с точки зрения безопасности и криптографических свойств, это не дает, а лишь усложняет реализацию (т.е. увеличивает сроки, стоимость разработки и т.п.), а также увеличивает вероятность несовместимости.

Автору неизвестно, чтобы существовал международный/европейский стандарт или техническая спецификация, где бы один криптографический алгоритм имел два объектных идентификатора для разных форматов кодирования параметров алгоритма (Big-Endian, Little-Endian), а тем паче для кодирования лишь части параметров.

Следует отметить, что подобная «многовекторность» не является главной причиной, но любое необоснованное, как крайне необходимое для целей безопасности/ криптографической стойкости, усложнение реализации алгоритма - это:

а) дополнительные затраты на создание и дальнейшее поддержание/ обслуживание алгоритма/ криптографического средства;

б) увеличение возможных ошибок и несовместимости, особенно при недостаточном уровне тестирования, о чем говорилось выше (см. Проблему №2. Низкий уровень стандартизации НСЭЦП. Тестирование соответствия в сфере КЗИ).

Вывод: При создании технических спецификаций не следует стараться «угодить» всем разработчикам, даже «влиятельным», а следует руководствоваться исключительно стандартами и передовой международной и европейской практикой.

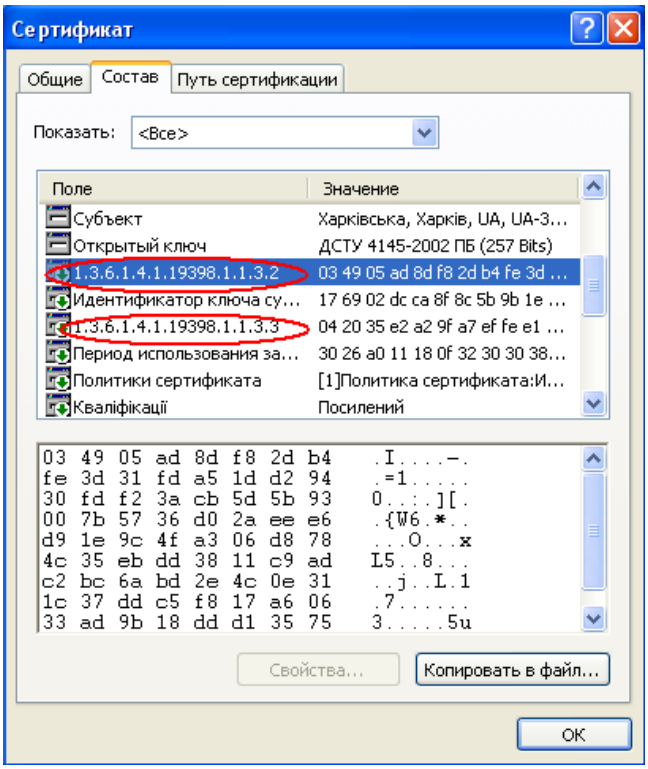
2) Создание криптографических объектов типа «2в1» (два в одном)

Стандартами X.509 определяется структура сертификата открытого ключа, обязательные и дополнительные/ опциональные атрибуты и расширения сертификата. Стандартами X.509 разрешается добавлять к структуре сертификата собственные расширения разработчика, не определенные стандартами. В этом случае, конечно, содержание таких расширений неизвестно никому (что это и что с ним делать, как обрабатывать …?), кроме самого разработчика, а потому такие расширения вообще не должны рассматриваться для интероперабельных систем.

Но... Несколько разработчиков в Украине, и соответственно несколько аккредитованных центров сертификации ключей (АЦСК), создали и используют X.509 сертификаты цифровой подписи с собственными расширениями, не определенными стандартами или официальными/ публичными спецификациями (причем эти расширения существенно влияют на обработку цифровой подписи/шифрование), что является нарушением принципов интероперабельности.

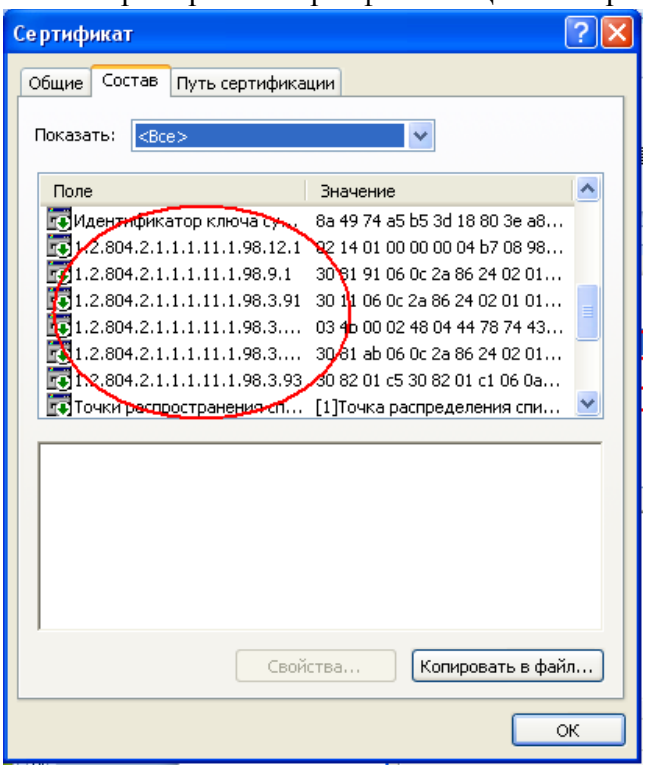
Отдельные разработчики разместили в этих расширениях ключи шифрования, т.е. в одном сертификате фактически содержится два открытых ключа - один для подписи, второй для шифрования (поэтому назовем такие объекты «2в1»):

Пример №1. Сертификат АЦСК в Украине:

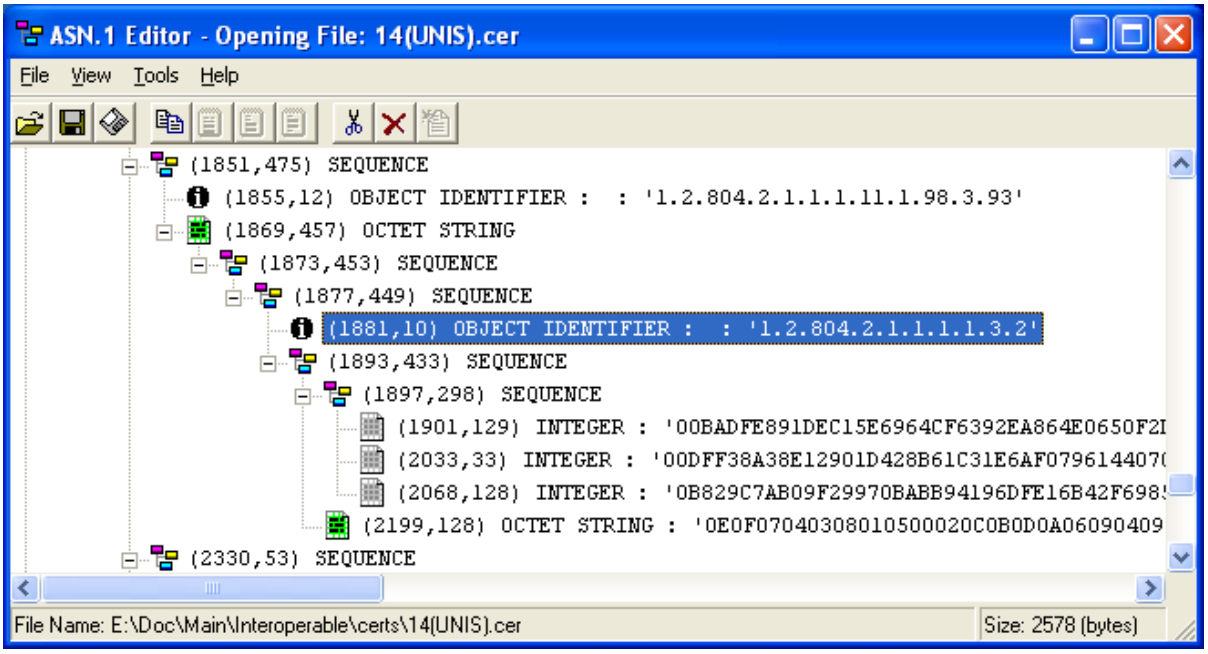


В этом сертификате присутствуют расширения с такими объектными идентификаторами (OID): 1.3.6.1.4.1.19398.1.1.3.2, 1.3.6.1.4.1.19398.1.1.3.3, которые не описаны в стандартах или спецификациях, не зарегистрированы надлежащим образом, а потому, содержание и назначение этих расширений неизвестно.

Пример №2. Сертификат АЦСК в Украине:



Например, расширение с OID =1.2.804.2.1.1.1.11.1.98.3.93 имеет такое значение:



Так как OID = 1.2. 804.2.1.1.1.1.3.2 означает алгоритм подписи ГОСТ 34.310-95 с хэш-функцией ГОСТ 34.311-95 (Gost34310WithGost34311) (см. [40]), то можно предположить, что в расширении размещены параметры алгоритма подписи ГОСТ 34.310-95 с хэш- функцией ГОСТ 34.311-95. Но сам сертификат выдан на открытый ключ, который имеет алгоритм с OID = 1.2.804.2.1.1.1.1.3.1.1, т.е. ДСТУ 4145-2002 с длиной ключа 307 бит. Итак, один сертификат открытого ключа содержит два ключа - ГОСТ 4145 и ГОСТ 34.310. Назначение и правила обработки второго ключа неизвестны.

Рассмотрим насколько подобная практика «2в1» отвечает стандартам X.509. В соответствии со стандартами X.509, в частности RFC 5280:2008 [22]:

1. Сертификат удостоверяет и регистрирует один открытый ключ, который содержится в поле PublicKey.
2. ЦСК должен проверять уникальность открытого ключа и то, что этот ключ связан с соответствующим ему личным/приватным ключом (PrivateKey).
3. Сертификат в поле KeyUsage содержит информацию об использовании (назначении) ключа PublicKey - для подписи, шифрования и т.п.
4. Рекомендуется устанавливать срок ключа шифрования не более одного года, а срок ключа подписи 1-2 года.

В случае размещения в расширении сертификата второго ключа (ключей), эти положения стандарта не могут быть применены для второго ключа (ключей), а потому этот дополнительный ключ(и) не может считаться действительным(и).

Вывод: Наличие неизвестных расширений, которые требуют обработки во время формирования подписи/ проверки подписи/ зашифровывания/ расшифровывания, является недопустимым для интероперабельных систем, независимо от алгоритма открытого ключа сертификата (ДСТУ 4145, RSA, ECDSA и т.п.).

3) Отсутствие технических спецификаций шифрования

Одной из причин, которая породила ошибочную практику «2в1», о которой говорилось в предыдущем пункте, является отсутствие технических спецификаций шифрования на открытых ключах ДСТУ 4145-2002. В данный момент такая техническая спецификация уже создана, хотя еще не введена в практическую деятельность АЦСК, а потому, проблема все еще существует.

Отсутствие технических спецификаций шифрования в сочетании с практикой «2в1» привела к тому, что каждый АЦСК предоставлял пользователям собственные («собственного видения/ понимания») алгоритмы шифрования и соответствующие библиотеки функций собственного формата (с интерфейсами «собственного видения/ понимания»).

Вместо того, чтобы принять меры относительно формулирования общих правил для всех разработчиков путем создания соответствующих технических спецификаций интероперабельности, в системах электронной отчетности (например, ГНА Украины) решили проблему иначе - путем создания ведомственного шлюза, который соединит в себе множество библиотек «собственного видения/ понимания» разработчиков АЦСК.

Поддерживать и сопровождать на любом шлюзе множество библиотек различных производителей - это, мягко говоря, не лучшая практика.

Вывод: Внедрить Технические спецификации шифрования на открытых ключах ДСТУ 4145-2002. Не может и не должно существовать необходимость в любых шлюзах, если все АЦСК будут соответствовать единым стандартам шифрования. Без этого интероперабельность невозможна, независимо от алгоритма ключа/ сертификата (ДСТУ 4145, RSA, ECDSA и т.п.).

4) Отсутствие технических спецификаций хранилища ключей/ сертификатов

Хранилище ключей и сертификатов предназначено для безопасного хранения закрытых ключей и соответствующих сертификатов на носителях информации. При этом под хранилищем ключей понимают именно файловое хранилище (программная реализация криптографического модуля), а не какую-либо аппаратную реализацию криптографического средства. Вопрос взаимодействия с хранилищами ключей и сертификатов является неотъемлемой составляющей интероперабельности.

При создании ведомственного шлюза (пример ГНА) дополнительно, для того чтобы была возможность выполнять криптооперации в обеих направлениях (клиент-шлюз, шлюз-клиент), необходимо на шлюзе также иметь **личные/закрытые ключи** каждого АЦСК (напомним – из-за несовместимости форматов «2в1» и алгоритмов шифрования).

Стараясь хотя кое-как упорядочить работу с различными библиотеками разных разработчиков, ГНА утверждает Унифицированный формат транспортного сообщения [44], в приложении 3 которого содержится «Спецификация криптографических функций». Но...

В параметрах указанных криптографических функций есть такие: «*Буфер з секретним ключем*», «*Буфер з сертифікатом*», но отсутствуют функции поиска и/или получения этих «*буферов*» (откуда они будут браться?).

Таким образом, на сегодняшний день в системе электронной отчетности ГНА необходимо:

1. Получить от всех разработчиков АЦСК библиотеки криптографических функций и интегрировать их в шлюз.
2. Создать возле (в зоне доступа) шлюза безопасные хранилища ключей и сертификатов (по количеству АЦСК или типов АЦСК по количеству разработчиков).
3. Каким-то образом (не определенным в Спецификациях) получать «*Буфер с секретным ключом*» для передачи его криптографической функции на выполнение операции.

Итак, ГНА сделало первый шаг к унификации, создав Спецификации, но оставило без унификации хранилища ключей и сертификатов, как и процедуры/ функции обращения к ним.

Существует лишь один международный стандарт, который применяется для хранилища ключей и сертификатов в виде файла (файловое хранилище) – это стандарт PKCS#12 [40],

который для внутреннего хранения ключей использует PKCS#8, а также PKCS#5, PKCS#9 и другие стандарты.

Для аппаратных, программно-аппаратных криптографических модулей стандарты форматов хранилищ отсутствуют; стандартами требуется обеспечение уровня безопасности хранения и функционирования. Для таких средств стандартизируются открытые интерфейсы (см. следующий пункт, стандарт PKCS#11). Следует отметить, что для аппаратных, программно-аппаратных средств хранилище может быть создано в любом формате, который разработчик считает лучшим и самым безопасным. Но в этом случае должны стандартизироваться открытые интерфейсы.

Кроме хранилищ типа PKCS#12 существует также хранилища Microsoft Windows, формат которых, вероятно, определен спецификациями Microsoft, которые не имеют статуса стандартов.

Стандарт PKCS#12 используется для резервирования (резервного копирования) ключей и сертификатов с их последующим импортом в программные, программно-аппаратные, аппаратные криптографические модули.

Использование хранилищ формата PKCS#12 распространенно в Java JVM, Linux/Unix операционных системах, но его главное назначение вытекает из названия стандарта «Personal Information Exchange Syntax» (Синтаксис обмена персональной/ личной информацией), т.е. для обмена. Следует отметить следующие недостатки/ уязвимости файловых хранилищ:

- Отсутствие защиты от копирования;
- Отсутствие защиты от атаки «грубой силы» (brute force attack);
- Во время выполнения криптографических операций личный/секретный ключ покидает «устройство», т.е. хранилище, и передается функциям выполнения операции, что может нарушить безопасность ключа.

Из-за этого файловое хранилище используется, как правило (из соображений безопасности):

- для резервирования (резервного копирования) или обмена (экспорта/ импорта) ключей и сертификатов;
- на защищенных компьютерах (в защищенной среде), где есть достаточные гарантии безопасного использования ключей.

В отдельных публикациях относительно интероперабельности НСЭЦП также обсуждается проблема хранилища ключей, например [45], но выводы, которые были сделаны, являются неверными. Так в указанной публикации предлагается:

«*Более того, для внутренней интероперабельности на территории Украины, не говоря уже о кроссертификации, необходим стандартный формат личного ключа, например, на основе де-факто стандарта PKCS#8*»

Во-первых, к кроссертификации вопрос формата личного ключа не имеет никакого отношения - на кросссертификацию передается X.509 сертификат, а не личный ключ (который, напомним, не должен покидать криптографический модуль).

Во-вторых, используя формат PKCS#8 личного ключа на уровне прикладных программ (отчетности и т.п.), якобы с целью интероперабельности, мы тем самым передаем на этот уровень (прикладной) непосредственно сам личный/ секретный ключ (его значение), из-за чего теряем любой контроль над ключом. Итак, автоматически такой криптографический модуль не может быть «Безопасным средством создания подписи», как этого требует Директива 1999/93/ЕС. Такой ошибочный, как представляется, подход существует и в решении ГНА, где требуется «*Буфер с секретным ключом*». О том, что интероперабельность и безопасность по сути являются антагонистическими требованиями, говорилось в начале этой публикации. Часто, и даже слишком часто, на практике при создании автоматизированных систем строится определенный концепт функциональности и интероперабельности без единой

мысли относительно безопасности. Для справки: безопасные средства создания подписи никогда (ни при каких условиях) не должны передавать на прикладной уровень (за границы криптографического модуля, программного, программно-аппаратного, или аппаратного) значение личного ключа. Операционное взаимодействие осуществляется при помощи так называемых дескрипторов (идентификаторы/ алиасы/ псевдонимы) закрытого ключа, а сам ключ, его значение, при этом не покидает границы криптографического модуля. Только при этих условиях криптографический модуль считается безопасным.

В-третьих, формат PKCS#8 личного ключа не содержит никакой информации о соответствующем ему (этому ключу) открытом ключе и сертификате, а потому нет возможности установить однозначное соответствие личного ключа и его открытого ключа/ сертификата. В этом случае даже стандартизация формата личного ключа и сертификата не даст интероперабельности, так как механизм соответствия личного ключа сертификату остается неопределенным. Итак, снова разработчики АЦСК «на собственное усмотрение/ понимание» будут реализовывать его, и, конечно же, каждый по-своему, так как соответствующего стандарта не существует.

Для информации: Microsoft по-своему реализует механизм соответствия ключа сертификату; в стандарте PKCS#12 это реализовано через алиасы/ псевдонимы (aliases); в стандарте PKCS#11 это реализовано с помощью внутреннего идентификатора объекта ID, который является общим для группы объектов закрытый ключ - открытый ключ - сертификат.

Вывод: Без унификации и стандартизации хранилища ключей и сертификатов, интероперабельность будет проблематичной, а без стандартизации процедур/ функций обращения к ключам и выполнения криптоопераций, интероперабельность невозможна независимо от алгоритма ключа/ сертификата (ДСТУ 4145, RSA, ECDSA и т.п.).

5) Отсутствие открытости интерфейсов

Для программных, программно-аппаратных криптографических модулей стандартизируются открытые интерфейсы, определенные стандартом PKCS#11 [40]. Ни один известный производитель подобных средств (не украинских) не поставляет их на рынок, не обеспечив реализацию стандарта PKCS#11.

Открытость интерфейсов достигается также путем создания так называемых Криптографических сервис-провайдеров (Cryptographic Service Provider, CSP), создание которых, как правило, базируется на интерфейсе PKCS#11, т.е. как надстройка над PKCS#11. В этом случае для интероперабельности могут использоваться как PKCS#11, так и более высокий уровень интеграции - CSP.

Существует де-факто два типа реализаций CSP: Microsoft CSP и Java CSP (JCA/JCE). Почти все известные производители криптографических средств (не украинских) поставляют их на рынок, обеспечив реализацию Microsoft CSP и Java CSP (JCA/JCE). А так как иностранные производители соответственно реализуют международные алгоритмы подписи/ шифрования, то именно этим и достигается требование нтероперабельности для международных алгоритмов. Т.е., проблема заключается не в использовании конкретно ДСТУ 4145 или RSA (см. вывод в публикации [47]), а в уровне качества изделия и соответствии стандартам, в частности, относительно открытых интерфейсов. Т.е., если реализовать RSA или другие международные алгоритмы, но с тем же уровнем «качества» («на собственное усмотрение/ понимание» разработчика), то получим такой же уровень неоперабельности, который имеется сегодня с ДСТУ 4145.

Следует подчеркнуть, что открытые интерфейсы, определенные стандартом PKCS#11, могут применяться не только для аппаратных/ программно-аппаратных, а и для чисто программных криптографических модулей.

Вывод: Без унификации и стандартизации открытых интерфейсов криптографических модулей интероперабельность невозможна, независимо от алгоритма ключа/ сертификата (ДСТУ 4145, RSA, ECDSA и т.п.).

Так или иначе, в основе указанных выше причин неинтероперабельности НСЭЦП лежит несоблюдение главных принципов интероперабельности [2]: следование стандартам и открытость интерфейсов. Итак, независимо от того, какой конкретно алгоритм/ набор алгоритмов, международных/ национальных и т.п., будет использоваться для ЭЦП, без устранения указанных причин НСЭЦП и в дальнейшем будет оставаться неинтероперабельной.

Общий вывод: Для практического достижения интероперабельности НСЭЦП Украины необходимо выполнить следующее:

1. Внести изменения в Закон Украины «Об электронной цифровой подписи», приведя его в соответствие с Директивой 1999/93/ЕС;
2. Создать открытые методики и наборы тестовых векторов для тестирования соответствия в сфере криптографической защиты информации; регламентировать процесс и критерии оценивания;
3. Активизировать работу относительно создания технических спецификаций, которые базируются на международных и европейских стандартах;
4. Поднять на качественно новый уровень работы по адаптации международных/ европейских стандартов по информационным технологиям и криптографической защите;
5. Безотлагательно принять практические меры относительно (технико-технологического) присоединения и внедрения в Украине европейской программы IDABC (Интероперабельное предоставление услуг европейского электронного правительства государственным администрациям, бизнесу и гражданам) путем внедрения соответствующих стандартов;
6. Запретить разработку/ создание любых ведомственных технических спецификаций теми государственными учреждениями/ ведомствами, которые не являются ответственными за это направление и не имеют соответствующей квалификации.

P.S. Эта публикация является оценочным суждением, убеждениями, критической оценкой определенных фактов и недостатков текущего состояния НСЭЦП Украины, которые выражены как субъективное мнение автора, соответственно Закону Украины «Об информации» и Конституции Украины относительно права на свободу мысли и слова, на свободное выражение своих взглядов и убеждений. Эта публикация не имеет целью унижения чести и достоинства, деловой репутации какого-либо лица, а касается исключительно интересов обеспечения профессиональности интероперабельности НСЭЦП Украины.

Перечень литературы

1. CEC. Commission of the European Communities, Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (1991) - Official Journal L 122 , 17/05/1991 P. 0042 - 0046;
2. IDABC. Enterprise & Industry DG, European Interoperability Framework for panEuropean e-government services, version 1.0, - Luxembourg: Office for Official Publications of the European Communities, Brussels, 2004, ISBN 92-894-8389-X;
3. SAGA. Standards and Architectures for e-government Applications – KBSt[11] Publication Series, ISSN 0179-7263, Volume 59, December 2003;
4. FIPS PUB 140-2 Security Requirements for Cryptographic Modules - Information Technology Laboratory National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8900, Issued May 25, 2001;

[11] KBSt (Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung) - Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KBSt), Координаційне та консультативне агентство федерального уряду з інформаційних технологій у Федеральній адміністрації/ Федеральному управлінні.

5. ISO/IEC 15408-1:2009 -- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model - 2009-12-03;
6. ISO/IEC 15408-2:2008 -- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components - 2008-08-19;
7. ISO/IEC 15408-3:2008 -- Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components - 2008-08-19;
8. ДСТУ CWA 14365-2:2009 - Настанова щодо використання електронних підписів. Частина 2. Профіль захисту для програмних засобів створення підпису (CWA 14365-2:2004, IDT), - Дата введення в дію: 01.07.2011;
9. ДСТУ CWA 14167-3: 2008 - Криптографічний модуль для послуг генерування ключів провайдером послуг сертифікації. Профіль захисту CMCKG-PP (CWA 14167-3:2004, IDT), - Дата введення в дію: 01.01.2010;
10. ДСТУ-П CWA 14172-5:2008 - Настанова Європейської Ініціативи стандартизації електронних цифрових підписів з оцінювання відповідності. Частина 5. Безпечні засоби створення підпису (CWA 14172-5:2004, IDT), - Дата введення в дію: 01.01.2009;
11. ДСТУ-П CWA 14172-6:2008 - Настанова Європейської Ініціативи стандартизації електронних цифрових підписів з оцінювання відповідності. Частина 6. Засіб створення підписів, що підтримує підписи, крім кваліфікованих (CWA 14172-6:2004, IDT), - Дата введення в дію: 01.01.2009;
12. ДСТУ-П CWA 14172-7:2008 - Настанова Європейської Ініціативи стандартизації електронних цифрових підписів з оцінювання відповідності. Частина 7. Криптографічні модулі, використовувані провайдерами послуг сертифікації для операцій підписування та послуг генерування ключів (CWA 14172-7:2004, IDT), - Дата введення в дію: 01.01.2009;
13. ДСТУ CWA 14355:2009 - Настанова щодо реалізації безпечних засобів створення підписів (CWA 14355:2004, IDT), - Дата введення в дію: 01.07.2011;
14. CWA 14169:2004 - Secure Signature-Creation Devices "EAL 4+";
15. CWA 14170:2004 - Security requirements for signature creation applications;
16. Директива 1999/93/ЄС Європейського парламенту та Ради «Про систему електронних підписів, що застосовується в межах Співтовариства» від 13 грудня 1999 року. – Офіційний переклад (http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_240);
17. Закон України «Про електронний цифровий підпис» від 22 травня 2003 року №852-IV - Відомості Верховної Ради України (ВВР), 2003, N 36, ст.276);
18. NIST. Public Key Interoperability Test Suite (PKITS). Certification Path Validation, Version 1.0, September 2, 2004;
19. NIST. Path Discovery Test Suite - Version 0.1.1, June 3, 2005;
20. The Advanced Encryption Standard Algorithm Validation Suite (AESAVS) November 15, 2002;
21. The XTS-AES Validation System (XTSVS) - Updated: March 2, 2011; Previously Updated: August 30, 2010; Original: March 31, 2010;
22. RFC 5280:2008 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
23. RFC 3279:2002 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
24. ДСТУ ETSI TS 102 176-1:2009 - Електронні підписи та інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції й асиметричні алгоритми (ETSI TS 102 176-1:2007, IDT);
25. ДСТУ ETSI TS 102 045:2009 - Електронні підписи та інфраструктури (ESI). Політика підписів для розширеної бізнес-моделі (ETSI TR 102 045 V1.1.1 (2003-03), IDT);
26. ISO 32000-1:2008 "Document management -- Portable document format -- Part 1: PDF 1.7",
27. ETSI TS 102 778 V1.1.1 (2009-04) - Technical Specification - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1
28. ETSI TS 102 778-1 V1.1.1 (2009-07) - Technical Specification - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES
29. ETSI TS 102 778-2 V1.2.1 (2009-07) - Technical Specification - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1
30. ETSI TS 102 778-3 V1.2.1 (2010-07) - Technical Specification - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles
31. ETSI TS 102 778-4 V1.1.2 (2009-12) - Technical Specification - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile
32. ETSI TS 102 778-5 V1.1.2 (2009-12) - Technical Specification - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures
33. ETSI TS 102 778-6 V1.1.1 (2010-07) - Technical Specification - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures
34. RFC 2119:1997 – Key words for use in RFCs to Indicate Requirement Levels;

35. ДСТУ ETSI TS 102 176-1:2004 Електронні підписи та інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції й асиметричні алгоритми;

36. ДСТУ ISO/IEC14888-1:2002 – Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення (ISO/IEC14888-1:1998, IDT);

37. ДСТУ ISO/IEC 10118-2:2003 Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції з використовуванням n-бітового блокового шифру;

38. CWA 14167-1:2003 - Security Requirements for Trustworthy Systems Managing. Certificates for Electronic Signatures - Part 1: System Security Requirements;

39. ДСТУ CWA 14167-2:2004 Криптографічний модуль для операцій підписання провайдером послуг сертифікації з резервним копіюванням - Профіль захисту CMCSOB PP;

40. PKCS #11 v2.20: Cryptographic Token Interface Standard - RSA Laboratories, 28 June 2004;

41. PKCS 12 v1.0: Personal Information Exchange Syntax – RSA Laboratories, June 24, 1999;

42. К. С. Борзілова. ЛІНГВІСТИЧНА ТЕОРІЯ. ТРУДНОЩІ ПРИ ПЕРЕКЛАДІ МОДАЛЬНИХ ДІЄСЛІВ - Вісник ЛНУ імені Тараса Шевченка № 9 (220), Ч. ІІІ, 2011;

43. НСЕЦП. Технічні специфікації форматів представлення базових об'єктів - 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 від 11 вересня 2006 р. № 99 /166;

44. Уніфікований формат транспортного повідомлення при інформаційній взаємодії платників податків і податкових органів в електронному вигляді телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису, наказ ДПА України від 12.07.2010 № 499;

45. Мелащенко Андрій Олегович, Перевозчикова Ольга Леонідівна. Тестовий стенд для інтероперабельності електронних цифрових підписів, - Наукові записки Києво-Могилянської академії. – К.: Видавничий дім „Києво-Могилянська академія", 2010. – С. 54-61;

46. А. О. Мелащенко, О. Л. Перевозчикова, РОЛЬ КОМПЛЕКТОВ ПОДПИСЕЙ В КВАЛИФИЦИРОВАННОЙ ИНФРАСТРУКТУРЕ ОТРЫТЫХ КЛЮЧЕЙ - Математичне та комп'ютерне моделювання, Серія: Технічні науки, Випуск 3, - 2010, стор. 138-154;

47. Мелащенко Андрей Олегович, Перевозчикова Ольга Леонидовна - Проблемы интероперабельности Национальной системы электронных цифровых подписей, - Кибернетика и системный анализ. – 2009. – № 3. – Р 55-63.

Эта публикация подписана цифровой подписью автора (martyn@itsway.kiev.ua). При этом использован ключ RSA, хотя может быть подписана каким-либо другим, в том числе ДСТУ 4145, или ECDSA, или др.

Мартыненко Сергей Васильевич

Подписано цифровой подписью: Мартыненко Сергей Васильевич
DN: cn=Мартыненко Сергей Васильевич, st=Киев, l=Киев, sn=Мартыненко, givenName=Сергей Васильевич, title=Директор технічний, email=martyn@itsway.kiev.ua, serialNumber=38
Дата: 2011.12.09 14:40:42 +02'00'