УДК 681.3:002.651.028(083.73)

КРОССЕРТИФИКАЦИЯ УКРАИНЫ

А.О. Мелащенко, О.Л. Перевозчикова

Институт кибернетики имени В.М. Глушкова НАН Украины,
03680, МСП, Киев, проспект Академика Глушкова, 40
тел. 526 3603, dep145@gmail.com

Проанализированы существующие способы кроссертификации с Евросоюзом, их технологические и организационные требования. Предложены меры для достижения внутренней интероперабельности в Украине для автоматической возможности кроссертификации с Евросоюзом.

Article deals with existing ways of crosscertification of Ukraine with the European Union, their technological and organizational requirements are analysed. Measures for achievement of internal interoperability in Ukraine for automatic possibility of crosscertification with the European Union are offered.

Использованные аббревиатуры

ЭЦП	Электронная цифровая подпись
PKI	Public key infrastructure (Инфраструктуру открытых ключей)
НСЭЦП	Национальная система электронных цифровых подписей
ТР	Технический регламент
СА	Certification authority (Орган сертификации)
ЦСК	Центр сертификации ключей
CTL	Certificate trust list (Список доверительных сертификатов)
PKCS	Public key cryptography standards (Стандарты криптографии открытого ключа)
ЦЗО	Центральний засвідчувальний орган
ВСА	Bridge certification authority (Орган мостовой сертификации, бридж)

Введение

Для интеграции Украины в ВТО, в целях евроинтеграции, развития внутреннего рынка и повышения доли экспорта необходимо внедрить в Украину нормы ООН и ВТО, и обеспечить их технологическую поддержку. Одни из основных компонентов технологической поддержки – ЭЦП, как инструмент обеспечения доверия (целостности и неопровержимости электронных документов). Поскольку реализации ЭЦП опираются на локальное законодательство и локальные технологические реализации, необходимо использовать механизмы признания двумя или большим количеством PKI-сертификатов открытых ключей и соответственно засвидетельствование определенными субъектами этих PKI правоспособности ЭЦП своих клиентов за территориальными границами (государственной границей) своей PKI, т. е. кроссертификацию.

Ныне в Украине поддержку ЭЦП обеспечивает НСЭЦП, гарантирующая от имени государства качество предоставляемых услуг. К сожалению, локальная реализация НСЭЦП не обеспечивает внутренней интероперабельности, а без нее невозможна кроссертификация. Для достижения внутренней интероперабельности необходимо принять в ближайшее время неотложные меры по созданию Технического регламента ЭЦП для организационного и технологического регулирования функционирования НСЭЦП. В ТР необходимо включить механизмы кроссертификации с мировым сообществом, в частности с ЕС, минимально модифицируя интероперабельную НСЭЦП, поскольку в Украине реализована европейская Директива [1] и гармонизированы европейские стандарты в ее поддержку.

В статье проанализированы известные способы кроссертификации с Евросоюзом, технологические и организационные требования. Предложены меры для достижения внутренней интероперабельности в Украине и автоматической возможности кроссертификации с Евросоюзом.

1. Механизмы кроссертификации

Корневые и связующие СА. Любому субъекту, желающему верифицировать сертификат, использованный в ЕЦП, необходимо знать, заслуживает ли доверия СА, издавший сертификат. Например, при получении подписи, основанной (как утверждается) на усиленном сертификате, как получатель может проверить, что СА контролируется или аккредитован согласно национальным нормам, а его услуги авторизованы на рынке? Есть несколько решений этой проблемы: корневой СА, связующий СА и список статуса доверия.

Корневой CA издает сертификаты подчиненных CA и ему непосредственно доверяют конечные пользователи подчиненных CA. Это означает, что, используя общий сертификат корневого CA, можно проверить все сертификаты пользователей, лежащие в корне иерархии. Понятие корневого CA не предусматривает, что корневой CA обязательно находится сверху любой иерархии, просто корневому CA доверяют непосредственно, по обыкновению с использованием самоподписанного "корневого сертификата", как это сделано в Украине на основании ее локального законодательства.

В нескольких странах основан общий корневой CA: в Германии RegTP (только для аккредитованных провайдеров услуг сертификации), в Нидерландах (только для правительственного использования), в Польше и Бельгии.

Многие эксперты считают, что значимость использования корневого CA переоценена. Это грубый инструмент для определения надежности и статуса CA, издающего сертификаты. Поэтому для бизнес-приложений стороны, полагающиеся на сертификат, чаще всего предпочитают определять непосредственно надежные CA, вместо того, чтобы полагаться на автоматизированную цепочку сертификатов.

Связанная с этим проблема – это политически значимый вопрос, кто отвечает за функционирование такого корневого CA и соответствует ли он каким-то стандартам? Эта проблема есть в Германии, где RegTP (как контролирующий и аккредитующий орган) также отвечает за управление корневым CA. К сожалению, корневой CA не полностью отвечает общим стандартам PKI, что привело к ситуации, в которой нельзя гарантировать интероперабельность между всеми провайдерами услуг сертификации, издающими усиленные сертификаты.

Альтернативная, но похожая технология обеспечения доверия через единый узел доверия – это концепция связующего CA. Главное отличие в сравнении с корневым CA состоит в том, что пользователь использует собственный CA (и его сертификат) как якорь доверия, вместо менее известного ему корневого CA. Каждый привлеченный CA потом кроссертифицирует связующий CA; так можно построить цепочку доверия сертификатов от собственного CA, через связующий CA, к сертификату любого конечного пользователя (юридического или физического лица).

Ныне в Европе есть несколько проектов связующих CA. Связующий CA развивала Єврокомисия в рамках программы IDA для использования государственными администрациями государств-членов ЕС. Проект "Европейского связующего CA" начали Дойчебанк с Дойчетелекомом, а затем поддержал TeleTrus (http://www.bridge-ca.org/). Хотя связующий CA может показаться более привлекательным, на самом деле он не решает потребности в детальной информации о статусе отдельного CA. Именно по этой причине в проекте связующего CA программы IDA модифицировали связующий CA, также поддерживающий списки доверия.

Список доверия – это подписанный список данных о CA и их статусе. В Италии правительство (т.е. AIPA) развило такую технологию довольно давно, чтобы распределить информацию о статусе аккредитации CA. Поэтому ETSI развил стандарт TS 102 231 [2] для предоставления согласованной информации о статусе CA для связующего CA в программе IDA.

Модель VA подтверждающего органа основана на использовании протокола OCSP, с помощью которого у сервера запрашивают статус проверяемых сертификатов. Каждая сторона, проверяющая статус полученного сертификата, обращается через защищенный онлайн-канал к серверу подтверждения, который возвращает текущую информацию о статусе сертификата и расположен в государстве-члене ЕС. Для сбора нужной информации в свою очередь он должен опрашивать другие сервера, возможно, расположенные в других государствах-членах, поэтому целесообразен центральный VA, чтобы обеспечивать информацией подтверждения каждый сервер. Поскольку предоставляется только статус, а не детали, то проверка цепочки подтверждения сертификата частично или полностью делегирована VA.

Некоторые государства-члены намерены развивать серверы подтверждения внутри администраций, чтобы они импортировали на сервер всю нужную информацию об удостоверяющих органах и регулярно ее обновляли. Тогда сервер может быстро и эффективно подтверждать сертификаты, а нагрузка, связанная с восстановлениями, будет приемлема, если есть эффективная инфраструктура внутренних сетей.

Модели иерархий PKI. *Иерархическая модель* PKI определяет доверительные отношения только в одном направлении. Как и в Украине, подчиненные CA не выпускают сертификатов своих вышестоящих CA. Вышестоящий CA навязывает условия, касающиеся типов сертификатов, которые может выпускать подчиненный CA. Государства ЕС однозначно отказались от этой модели, в Украине она уместна ввиду своей тривиальности и пока отсутствия полезного опыта реализации PKI как у разработчиков, так и у клиентов ЦСК.

Сетевая модель PKI определяет как пункты доверия все CA; именно поэтому пользователи будут доверять CA, который издал их сертификат. CA выпускают сертификаты друг другу; такая пара сертификатов описывает их двусторонние отношения доверия.

Модель доверия Web/Интернета основана на списках CTL доверия сертификатов, подписанных структурами данных PKCS № 7. Многие государства-члены ЕС заинтересованы в использовании CTL, подписанных BCA, как альтернативном механизме кроссертификации в сетевых моделях, имея возможность сохранить контроль над тем, каким сертификатам они доверяют. Эти структуры могут содержать список “доверенных CA”, идентифицированных в CTL с помощью выборки из открытого ключа сертификата рассмотренного CA. Также CTL содержит идентификаторы политик и поддерживают расширение.

С позиций внутридоменной интероперабельности по сути CTL заменяет пары кроссертификатов. Конкретная сторона доверяет издателю CTL, значит, доверяет CA, указанному в CTL.

Сначала CTL предназначали для кроссертификации без зависимости от каталогов, хотя их можно использовать для выражения любой другой политики относительно набора идентификаторов. Реализовав так называемые хранилища CTL, если цепочка сертификации начинается в корне, который не находится в корневом хранилище сертификатов, легко проверять CTL. Если выборка корневого сертификата найдена в CTL, то корень приемлем.

Модели кроссертификации. Ныне в мировой практике интенсивно создают так называемые связующие / шлюзовые CA (bridge/gateway CA. BGCA) для кроссертификации на международном уровне. Известнейшие проекты – Федеральный связующий удостоверяющий орган (FBCA) США и связующий / шлюзовой CA Еврокомиссии в рамках программы IDABC, которой с 2005 г. переданы полномочия программы IDA для взаимодействия между государственными администрациями стран Евросоюза. Для Украины целесообразен опыт последнего BGCA, поскольку его создают согласно положениям Директивы 1999/93/ЕС, в частности относительно манипулирования усиленными сертификатами открытых ключей. Уже разработан ряд нормативных документов (в частности ETSI TS 102 231 v3.1.1 от 2009 г. [2]) для проведения кроссертификации и рациональные технологические схемы организации трансграничного признания сертификатов и архитектурной модели связущего/шлюзового CA. Эти схемы в полной мере подходят для организации отношений НСЭЦП Украины с BGCA в рамках программы IDABC.

Подчеркнем, что НСЭЦП в Европе на 8–10 лет опережают украинскую. Однако Еврокомиссия признала недостатки и сложности, препятствующие построению общеевропейских связующих/шлюзовых CA. Среди них назовем не разнообразие трактовок Директивы 1999/93/ЕС в национальном законодательстве государств-членов, а низкая интероперабельность НСЭЦП на национальном уровне, поскольку в странах ЕС обычно существует не одна иерархия CA, а несколько, обслуживающих преимущественно транснациональные корпорации. Поэтому для присоединения к связующему/шлюзовому CA каждый корневой CA на свое усмотрение решает ряд задач, прежде всего опираясь на специфику применения своей PKI.

Укажем, что Украина пока не ощущает потребности во взаимодействии с субъектами транснациональных корпораций, способных построить PKI независимо от ЦЗО. Фирмы-резиденты Украины в составе транснациональных корпораций для корпоративного взаимодействия могут иметь заграничные сертификаты, а для взаимодействия с украинскими резидентами должны применять сертификаты НСЭЦП.

Среди применений ЭЦП в странах ЕС, кроме eGoverment, распространен eBanking, eTax для граждан и компаний, e-ID-карточки регистрации населения как удостоверения личности, цифровой нотариат и т.п. В Украине имеем законодательную базу лишь для электронного документооборота в органах государственной власти и местного самоуправления. Элементы eBanking реализованы в системах „клиент-банк” и системе конфиденциальной межбанковской связи Нацбанка Украины для электронной проводки банковских платежей. Эту систему НБУ развивает в соответствии с концепцией ЗЦ (укр. Засвідчувальний центр). Другие элементы eBanking задекларированы в Постановлении НБУ (зарегистрировано в Минюсте в январе 2005 г.) о Национальной системе массовых электронных платежей [3], в которой введено понятия смарт-карточки с аутентификацией, тем не менее четко не определены требования к механизмам ее реализации.

Модель связующего CA (рис. 1) называют PKI “hub-and-spoke”, поскольку BCA связывает много PKI в одном, известном центре. В сравнении с сетевым PKI, выявление цепочки сертификации упрощено в BCA PKI; вдобавок BCA PKI имеет более короткие цепочки доверия, чем сетевая PKI с таким же количеством CA. Тем не менее, как только одно государство-член ЕС подписалось на BCA, вопрос доверия переходит в ведение органа, который руководит / владеет этим BCA.

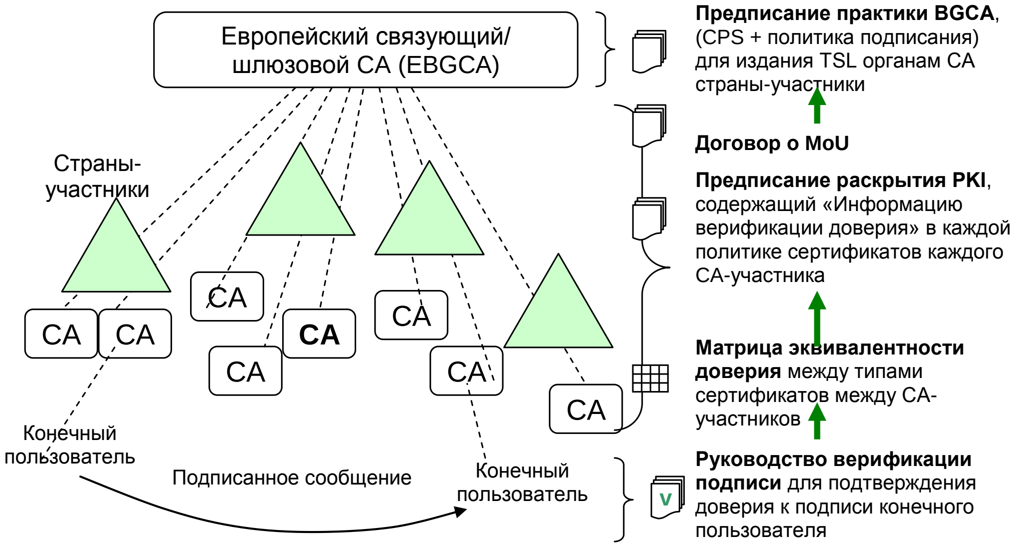

Рис. 1. Схема рекомендаций европейского связующего / шлюзового CA

Модифицированная модель BCA (рис. 2) (как комбинация модели доверия Web / Интернета и модели связующего CA) родилась по желанию многих государств-членов на собственное усмотрение отбирать сертификаты, которым они доверяют. Причем государства могут дополнять эту инфраструктуру открытым для госслужащих национальным удостоверяющим органом, если это допускают технические возможности.

Поскольку BCA расположен в Евродомене, он обеспечивает локальным доменам государств-членов один из вариантов: сертификаты открытых ключей национальных CA или список доверия сертификатов аккредитованных CA. В последнем случае:

- связующий CA распределяет список надежных корневых сертификатов, выполняющих общие требования;
- список подписывает своим сертификатом связующий CA;
- некоторые государства-члены просто на доверии воспринимают этот список;
- другие государства-члены могут создавать собственный список корней, которым они доверяют, удаляя некоторые сертификаты и переподписывая обновленный список собственными сертификатами.

Можно поддерживать секторные списки CTL по потребности, т.е. соединяя вместе сертификаты CA, установленные для пользователей этого сектора деятельности. Причем BCA должны обеспечивать:

- обмен и надлежащее восстановление кроссертификатов с "главным" CA каждой привлеченной PKI;
- регулярное (по требованию) направление членам списков доверия сертификатов (возможно, секторного CTL);
- службы каталогов, которые предоставляют сертификаты открытых ключей, выпущенные связующим CA для каждой привлеченной PKI, как и соответствующие списки отозванных удостоверяющих органов и списки отозванных сертификатов;
- эти службы каталогов необходимо обновлять хотя бы каждый день, желательно чаще;
- веб-сайт, публикующий списки CTL связующего CA и документы: Меморандум о согласии и описание политик сертификатов;
- опционально по запросу партнеров онлайн-верификацию статуса сертификатов через OCSP.

Руководящий орган BCA должен публиковать:

- технические интерфейсы для привлеченных PKI, чтобы взаимодействовать со связанными CA;
- тестовый стенд, помогающий претендентам проверить свой интерфейс на специальном веб-сайте.

Рис. 2. Заинтересованные стороны европейского связующего / шлюзового CA

2. Необходимые шаги для кроссертификации

С одной стороны, Закон Украины "Об ЭЦП" [4] гарантирует от имени государства качество услуг, которые предоставляет НСЭЦП. С другой – Украина является членом СОТ, диктующего правила eEconomy, соответственно eCommerce. "Доверие" (trust) eEconomy опирается на ЭЦП. Поэтому необходима интероперабельность НСЭЦП как внутри Украины, так и вне. Тут "интероперабельность" обеспечивает одинаковую трактовку базовых услуг и прав / обязательств пользователей / провайдеров относительно подписания договоров на предоставление услуг. Проблемы внутренней и внешней инетроперабельности НСЭЦП описаны в [5].

Еще один аспект НСЭЦП – формализованная процедура оценивания соответствия принятых технологических и организационных положений действующим национальным стандартам. Согласно Закону Украины "О стандартах" [6], необходимо иметь формализованные процедуры оценивания соответствия. Поэтому необходимы формализации организационной составной НСЭЦП, методики оценивания соответствия в поддержку Закона "Об ЭЦП" и Технического регламента НСЭЦП. Также необходимо уточнить методику оценивания соответствия, основываясь на принципах стандартизации, применимых институциями ЕС.

Общие положения. При формализации организационной составной и процедур аккредитации достигаем возможности кроссертификации, свободы передвижения услуг и "интероперабельности" организационной составляющей НСЭЦП. Украина имеет относительно слабую инвестиционную привлекательность, в частности ввиду запутанных правил налогообложения и бухгалтерского учета. Поэтому необходимо стандартизировать организационную составляющую и формализовать методики оценивания соответствия для минимизации согласований при кроссертификации и перехода клиента от одного провайдера услуг к другому (возможно, иностранному).

Минимальный необходимый набор для создания доверия, используя ЭЦП в eEconomy, состоит из Органа сертификации (в Украине – аккредитованный ЦСК), выдающего усиленные сертификаты, и Органа штемпелевания времени (в дальнейшем под словом "Орган" понимаем оба, см. рис. 3). Как правило, с органом(ами) клиент заключает договор на предоставление услуг, в котором указаны обязательства сторон и качество услуг. Кроме договора, каждый Орган имеет нормативные документы, на основании которых он функционирует и которые регламентируют конкретный уровень безопасности Органа. Таким образом, клиент обязан ознакомиться с набором нормативных документов, см. рис. 4. Подчеркнем, что внимание уделено точке зрения клиента, а относительно процедуры аккредитации Органа нужен более полный пакет документов.

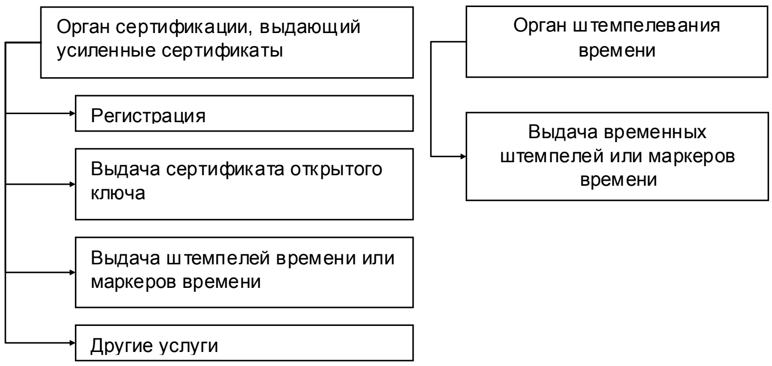

Рис. 3. Услуги базовых органов НСЭЦП

Рис. 4. Нормативные документы Органа (ЦСК) с позиций клиента

В гетерогенной среде eEconomy невозможно гарантировать, что *n* субъектов взаимоотношений будут пользоваться услугами одного общего Органа. Гарантия, которую аккредитованные Органы предоставляют одинаково качественные услуги, – это выполнение Закона Украины "Об ЕЦП" [4] и возможность кроссертификации, причем максимально достижимая для всех реализаций Директивы 1999/93/ЕС. Отсюда следует стандартизация политики Органов и формализация оценивания соответствия. Рис. 5 иллюстрирует стандартизацию политик Органов, причем НСЭЦП должны отвечать европейским стандартам и практике.

Серия стандартов ДСТУ-П CWA 14172 [7] (в 8 частях) гармонизирована с соответствующей серией, разработанной ЕС и формализовавшей оценивание соответствия, в частности ETSI TS 101 456 [8] и ДСТУ ETSI TS 102 023 [9]. При наличии спецификаций требований можно оценить их соответствие, что и сделали институты стандартизации ЕС и Орган сертификации федерального бриджа США (см. ДСТУ ETSI TR 102 458 [10]), показав полное соответствие политик для выполнения бизнес-транзакций с использованием ЭЦП.

В Украине разработано 3 из 5 стандартов в поддержку стандартизации организационной составляющей НСЭЦП. Нужно ввести эти нормы вместе со стандартизацией других частей НСЭЦП для выполнения Законов Украины и возможности кроссертификации, прежде всего со странами СОТ.

Рис. 5. Методика оценивания соответствия политик Органов стандартам

Формализация аккредитации ЦСК. Отсутствие стандартов и неспособность акторов рынка НСЭЦП создать согласованные спецификации сущностей привели к полному отсутствию интероперабельности НСЭЦП в Украине. Чтобы исправить ситуацию и построить НСЭЦП согласно эталонной модели QPKI, регламентирующей высококачественные услуги ЭЦП, следует на этапе аккредитации допускать только интероперабельные комплексы ЦСК. Эта возможность появилась недавно, после гармонизации части стандартов ЕС эталонной модели QPKI (см. ДСТУ ETSI TS 102 045 [11]). Формализация также нужна согласно Закону Украины "Об ЭЦП" для создания Технического регламента НСЭЦП.

Перед формализацией процесса аккредитации ЦСК классифицируем приемы формализации. Под классификацией понимаем уровень детализации требований и целесообразную верификацию. Требования разделены на две группы: экспертные оценки с формализованной процедурой оценки соответствия и тестовый стенд (программная реализация) на соответствие спецификациям базовых объектов НСЭЦП (табл. 1).

Таблица 1. Классификация приемов формализации и задействованные национальные стандарты Украины

	Название объекта	Тип оценки	Методика оценивания
1	Политика органа сертификации	Экспертные оценки	ДСТУ-П CWA 14172-2, ETSI TR 102 437
2	Политика органа штемпелевания времени	То же	ДСТУ-П CWA 14172-8
3	Надежные системы управления сертификатами	„-„	ДСТУ-П CWA 14172-3
4	Общие этапы верификации подписи	„-„	ДСТУ-П CWA 14172-4
5	Надежные средства создания подписи	„-„	ДСТУ-П CWA 14172-5
6	Криптомодули, используемые провайдерами услуг сертификации	„-„	ДСТУ-П CWA 14172-7
7	Формат сертификата открытого ключа	Программные тесты	Спецификации согласно ДСТУ ETSI TS 101 862
8	Формат личного ключа	То же	Спецификации согласно PKCS 12
9	Формат подписи	„-„	Спецификации согласно ДСТУ ETSI TS 101 733, ДСТУ ETSI TS 101 903, ДСТУ ETSI TS 102 734, ДСТУ ETSI TS 102 904
10	Протокол штемпелевания времени	„-„	ДСТУ ETSI TS 101 861
11	Формат токена временного штемпеля	„-„	ДСТУ ETSI TS 101 861

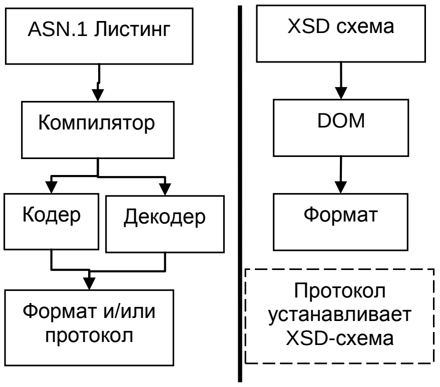

Рис. 6. Общая процедура создания формата или / и протокола

Тесты на интероперабельность. Рассмотрим реализацию тестового стенда (далее Стенд). Распределение оценок на экспертные и программные тесты введено для достижения интероперабельности в разных по своей природе средах. Первая сфера касается юриспруденции и безопасности, здесь невозможно (экономически нецелесообразно) формализовать все аспекты взаимоотношений между субъектами. Во второй технологической сфере без полной формализации субъектов и их взаимодействия невозможно достичь интероперабельности. Относительно технологического аспекта отношений речь идет о форматах и протоколах. Ныне их строят на основе ASN.1 [12] или в соответствии с XSD-схемой [13], общую процедуру см. на рис. 6

Для реализации базовых объектов НСЭЦП использовано оба механизма. Схожесть механизмов состоит в предоставлении языково- и платформо-независимой спецификации объектов. Эти спецификации декларируют национальные, гармонизованные с международными стандарты, также описывают ожидаемое поведение объектов. Поскольку де-факто есть множество способов реализовать указанные спецификации и ожидаемое поведение объектов, необходимо создать стенд, контролирующий соответствие реализаций установленным форматам и ожидаемому поведению объектов. Итак, имеем схему, приведенную на рис. 7.

Стенд – это набор программных тестов для специальных и/или контрольных испытаний разнообразных объектов для достижения интероперабельных реализаций базовых объектов НСЭЦП. Тесты (соответственно объекты и / или их части) разделены на две группы: специальные и контрольные. Это обусловлено уровнем требований в стандартах "обязательные" и "опциональные". Примером может служить согласно RFC 5280 опциональное поле "subjectAltName" сертификата открытого ключа, содержащее псевдоним владельца.

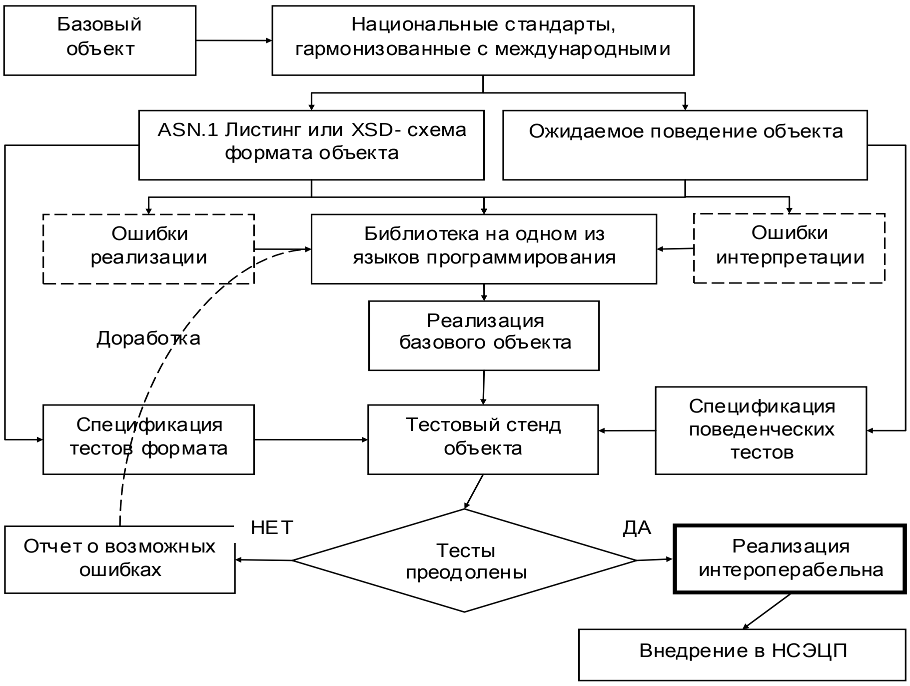

Рис. 7. Общая схема функционирования тестового стенда НСЭЦП

Сертификаты соответствия. По Закону Украины «Об ЭЦП» средства криптозащиты должны иметь сертификат соответствия или позитивное экспертное заключение. Этот пункт Закона является несомненным юридическим препятствием кроссертификации НСЭЦП, поскольку в результате применения признанных в мире методик оценки соответствия в Евросоюзе независимые оценщики качества сертифицируемой продукции выдают только «сертификаты соответствия», а поддержанная в Украине альтернатива «позитивное экспертное заключение» действует только на территории Украины.

При кроссертификации НСЭЦП необходимо юридически доказать технологическую и организационную зрелость ЦСК, посредством сертификатов соответствия. Ныне в Украине все 12 аккредитованных ЦСК имеют, только позитивные экспертные заключения, т.е. не могут пройти кроссертификацию в рамках Евросоюза. Усугубляет ситуацию невозможность признания в Украине полученных европейских сертификатов соответствия без специального межгосударственного соглашения.

Для достижения внутренней и внешней интроперабельности НСЭЦП и возможности кроссертификации необходимы изменения в Законе Украины «Об ЭЦП», закрепляющие единственный путь оценки соответствия с получением «сертификата соответствия» [14]. Для такой ресурсоемкой процедуры необходимо заключить межгосударственного соглашения с ЕС о взаимном признании сертификатов соответствия для создания интероперабельных и признаваемых в мире продуктов, в частности для ЭЦП.

Выводы

Для выполнения требований Закона Украины "Об ЭЦП" и кроссертификации необходимо добиться интероперабельности НСЭЦП Украины, т.е. задействовать жесткую процедуру аккредитации, которая отбрасывает неинтероперабельные реализации программно-технических комплексов, библиотек и т.п. Такую процедуру аккредитации целесообразнее строить на основе серии ДСТУ-П CWA 14172 (в 8 частях) и спецификаций тестов интероперабельности согласно ETSI-стандартам эталонной бизнес-модели QPKI.

Необходима новая редакция Закона Украины "Об ЭЦП", допускающая только сертификаты соответствия. Целесообразно межгосударственное соглашение с ЕС о взаимном признании сертификатов соответствия для признания зрелости всех составляющих НСЭЦП (как ЕС, так и Украины).

Единственным нормативным и минимаксным способом достижения интероперабельности НСЭЦП является Технический регламент. Но при его создании одной из целей должна быть кроссертификация со всей планетой, в частности с ЕС. Без учета этого можно повторить ошибку 2005 г., когда построение НСЭЦП пошло по пути, отличном от международной стандартизации. Ныне имеем реальную возможность учета опыта ЕС для кроссертификации посредством интеграции тестового стенда европейского Bridge-CA для поддержки внутренней интероперабельности согласно положениям Технического регламента и автоматической кроссертификации с ЕС.

1. *Директива* 1999/93/ЕС Европарламента и Совета от 13 декабря, 1999 г. о среде сообщества электронных подписей.
2. *ETSI* TS 102 231 V3.1.2 (2009-12) Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information.
3. *Правила* Національної системи масових електронних платежів, затверджені постановою Правління Національного банку України від 10.12.2004 № 620.
4. *Закон* України від 22.05.2003, № 852-15 «Про електронний цифровий підпис».
5. *Мелащенко А.О., Перевозчикова О.Л.* «Проблемы интероперабельности Национальной системы электронных цифровых подписей» // Кибернетика и системный анализ. – 2009. – № 6. – С. 55–63.
6. *Закон* України від 01.12.2005 № 3164-IV «Про стандарти, технічні регламенти та процедури оцінки відповідності».
7. *ДСТУ*-П CWA 14172:2008 Настанова EESSI з оцінювання відповідності.
8. *ETSI* TS 101 456 Електронні цифрові підписи та інфраструктури. Вимоги до політики органів сертифікації, які видають кваліфіковані сертифікати.
9. *ДСТУ* ETSI TS 102 023 Електронні підписи й інфраструктури (ESI). Вимоги політики для органів штемпелювання часу.
10. *ДСТУ* ETSI TR 102 458 Електронні підписи й інфраструктури (ESI). Таблиця відповідності між американською федеральною політикою сертифікації з'єднувального органа (bridge-CA) та європейською політикою посиленого сертифіката (TS 101 456).
11. *ДСТУ* ETSI TS 102 045 Електронні підписи й інфраструктури (ESI). Політика підписів для розширеної бізнес-моделі.
12. *ДСТУ* ISO/IEC 8825-1:2008 Інформаційні технології. ASN.1 правила кодування».
13. *W3C* Recommendation 28 October 2004 «XML Schema».
14. *Закон* України від 01.12.2005 № 3164-IV «Про стандарти, технічні регламенти та процедури оцінки відповідності».