УДК 681.3

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ВОПРОСЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ ЭЦП

Даниил Мялковский, Алексей Скиба
ДСТСЗИ СБ Украины

Анотація: **Розглядаються деякі організаційно-технічні аспекти побудови та функціонування національної системи електронного цифрового підпису, в тому числі структура системи, функції та обов'язки її суб'єктів, питання стандартизації і сумісності форматів даних, криптографічних протоколів тощо.**
Summary: **In this article are considered some organizing-technical aspects of the building and operating the national system of the electronic digital signature, including structure of the system, functions and duties its subject, questions to standardizations and compatibility data format, cryptographic protocol and etc.**
Ключові слова: **Електронний цифровий підпис, сертифікат ключа, центр сертифікації ключів, центр реєстрації, загальнодоступний каталог, національна інфраструктура відкритих ключів, центральний засвідчувальний орган, засвідчувальний центр.**

Оставляя в стороне вопросы юридического характера, связанные с правовыми вопросами использования электронной цифровой подписи (ЭЦП), рассмотрим некоторые технические аспекты национальной инфраструктуры с открытым ключом (НИОК), в частности общую технологию функционирования, взаимодействие в этой инфраструктуре конечных пользователей с поставщиками услуг ЭЦП, а также вопросы стандартизации и совместимости различных криптографических приложений и протоколов.

Анализ этих вопросов основывается на редакции проекта закона "Об электронной цифровой подписи", принятого в первом чтении, тексте законопроекта, подготовленного для вынесения на последующее чтение, а также общей технологии применения цифровой подписи в глобальных сетях с неограниченным количеством пользователей.

В основе использования механизмов ЭЦП на основе асимметричных криптографических преобразований лежат открытые и секретные ключи. Как известно, секретный ключ используется для наложения цифровой подписи, открытый – для ее проверки. В силу тех или иных причин требуется их смена, отзыв, распределение и т. д. Если речь идет о нескольких пользователях небольшой организации, то эти операции, как правило, совершаются "вручную" администратором системы безопасности. Если же пользователей сотни и более, то процесс управления ключами становится очень сложным и громоздким. Вероятность ошибок в таком случае сильно возрастает, что непременно приведет к снижению уровня безопасности в целом. Когда же речь идет о больших корпоративных и глобальных сетях, где имеют место тысячи и более пользователей, которые зачастую не имеют личного контакта или гарантированного безопасного канала обмена открытыми ключами, организовать процесс управления ключами "вручную" практически невозможно. Для решения этих проблем требуется создание специальной системы или инфраструктуры поддержки управления ключами, в основе которой лежит независимый специальный субъект, ответственный за управление ключами в общей инфраструктуре (в терминах законопроекта – центр сертификации ключей).

Общепринятым названием этой системы, которое используется в иностранной литературе, является инфраструктура открытых ключей (Public Key Infrastructure).

Инфраструктура открытых ключей (ИОК) представляет собой комплекс программно-аппаратных средств и организационно-технических мероприятий, необходимых для использования асимметричных криптографических схем в прикладных сферах, где могут использоваться механизмы ЭЦП.

Таким образом, основной целью создания и функционирования ИОК является обеспечение безопасного обмена открытыми ключами между участниками электронного взаимодействия.

Структурно ИОК состоит из субъектов и объектов, а также нормативных документов, которые регламентируют порядок работы субъектов и использование объектов ИОК (политика сертификации, политика безопасности, профайл (формат) сертификата и списков отозванных сертификатов и т. д.). К субъектам относятся центры сертификации ключей, центр регистрации, общедоступные каталоги или сетевые справочники, конечные пользователи. К объектам – сертификат ключа, документ (может быть в электронном или бумажном виде), который однозначно связывает определенное лицо (владельца сертификата) и его открытый ключ, подписанный ЭЦП независимой третьей стороной в информационном

обмене – (центром сертификации ключей), список отозванных сертификатов, сообщений “запрос на сертификат”, “компрометация сертификата”.

Функции, которые выполняет ИОК, условно можно разделить на основные (функции управления сертификатами) и дополнительные.

В состав основных функций входят:

регистрация (идентификация) конечного пользователя;

сертификация открытых ключей (процесс формирования сертификатов открытых ключей для конечных пользователей);

публикация (распространение) сертификатов в открытом каталоге для обеспечения доступа к ним субъектов взаимодействия;

отзыв сертификатов (процесс блокирования или отмены действия сертификата при условии возникновения определенных обстоятельств).

Обстоятельствами отзыва (аннулирования) или блокирования сертификата может быть компрометация секретного ключа конечного пользователя и прочие события.

К дополнительным функциям, которые выполняет ИОК, можно отнести:

взаимную сертификацию (кросс-сертификацию) центров сертификации ключей;

проверку легитимности сертификата;

архивацию сертификатов;

поддержку невозможности отказа от ЭЦП;

управление "историей" сертификатов;

“временные штампы”;

нотариальное засвидетельствование и т. д.

Современные тенденции развития национальной экономики, задачи сохранения единого экономического, финансового и информационного пространства на территории Украины диктуют необходимость создания инфраструктуры открытых ключей на национальном уровне. Такая национальная инфраструктура должна стать основой для обеспечения юридически значимого и безопасного информационного обмена по открытым сетям связи между всеми участниками информационного взаимодействия от органов государственной власти различных уровней, коммерческих организаций, до отдельных физических лиц.

Структура НИОК, а также функции и обязанности ее субъектов регламентируется законом “Об электронной цифровой подписи”.

НИОК создается в целях:

создания единой юридически значимой системы электронной идентификации субъектов информационного взаимодействия;

обеспечения безопасности информации при информационном взаимодействии;

создания надежной единой иерархической системы управления открытыми ключами средств цифровой подписи субъектов информационного взаимодействия;

создания и функционирования средств электронного нотариата (электронного заверения договоров), электронной коммерции и электронного ведения бизнеса.

Реализация такой системы в полном объеме позволит надежно гарантировать подлинность, целостность документов, а также, что очень важно, юридическую значимость электронного документооборота. Это, в свою очередь, повысит эффективность управления на всех уровнях и, что немаловажно, существенно повысит эффективность контроля за выполнением принятых решений.

Построение такой системы требует проведения ряда согласованных мероприятий организационного и технического характера.

К группе мероприятий технического характера следует отнести целый ряд задач, которые необходимо решить в области использования технологии ЭЦП и подготовки соответствующей информационно-технологической базы. В первую очередь здесь крайне важно определить формат сертификатов ключей и списка аннулированных сертификатов.

Структурно в НИОК входят субъекты, которые обеспечивают функционирование системы управления сертификатами, а также конечные пользователи.

НИОК включает следующие субъекты и компоненты.

1. Центр сертификации ключей (ЦСК), который обычно по функциональным, технологическим и территориальным признакам разделяется на технические компоненты: центр сертификации (ЦС), центр регистрации (ЦР) и сетевой справочник или общедоступный каталог.

2. Конечных пользователей – владельцев сертификатов открытых ключей.

3. Организатора НИОК – центрального удостоверяющего органа, который является корневым ЦСК и осуществляет техническое управление всей НИОК в целом.

Следует отметить, что деятельность ЦСК, т. е. деятельность по предоставлению услуг в сфере ЭЦП в соответствии с последней рабочей редакцией законопроекта не предусматривает предварительного получения лицензий или разрешений, кроме случаев добровольной аккредитации. Лицензированию подлежат разработка, производство, сертификационные испытания, тематические исследования, экспертиза, а также ввоз, вывоз средств цифровой подписи для коммерческой эксплуатации.

Центр сертификации предназначен для формирования и ведения базы данных, публикации сертификатов конечных пользователей и списков отозванных сертификатов.

Центр регистрации предназначен для обеспечения организационно-технических мероприятий, связанных с регистрацией и идентификацией конечных пользователей в системе. Он является единственной точкой взаимодействия конечного пользователя с компонентами системы. Сам ЦР не формирует сертификаты конечных пользователей, а только подготавливает необходимую информацию для ЦС и обеспечивает взаимодействие с ним. Кроме этого, ЦР обеспечивает получение и обработку сообщений о компрометации ключей конечных пользователей и осуществляет оперативное оповещение пользователей обо всех изменениях, происходящих в ЦСК (компрометация ключей, плановая смена ключей и т. п.). Центры регистрации также могут выполнять дополнительные функции, такие как разбор конфликтных ситуаций, доказательство авторства электронного документа, подписанного ЭЦП и т. д.

Сетевой справочник (СС) или общедоступный каталог является одним из компонентов ЦСК и предназначен для хранения, распространение сертификатов и списков отозванных сертификатов, сформированных данным ЦСК. В качестве справочника сертификатов в основном используется сервис, основанный на протоколе LDAP, а также службы с протоколами доступа HTTP, FTP.

Конечными пользователями в соответствии с законопроектом могут быть как физические, так и юридические лица, в отличие, например, от соответствующего российского закона, который исключает из пользователей юридические лица.

Глобальные по масштабу ИОК национального уровня имеют большое количество ЦСК (от нескольких десятков до нескольких сотен), а также неограниченное количество конечных пользователей (до нескольких миллионов). Такие инфраструктуры должны обеспечивать возможность проведения защищенного взаимодействия и установления доверия между пользователями, которые являются клиентами разных ЦСК. Для решения этой проблемы существует несколько базовых концептуальных моделей общей службы ИОК, таких как иерархическая, сетевая и мостовая.

Законопроектом “Об электронной цифровой подписи” определяется наиболее распространенная – иерархическая модель сертификации открытых ключей, основанная на иерархии ЦСК, которая начинается от единого корня. В общем случае, все ЦСК подчинены корневому ЦСК. Корневой ЦСК осуществляет регистрацию ЦСК и формирует для них сертификаты (корневые сертификаты). ЦСК в свою очередь формируют сертификаты другим ЦСК и конечным пользователям. Глубина иерархии не ограничивается. Корневой ЦСК формирует личный сертификат ключа и подписывает его с помощью собственного секретного ключа.

Преимуществом иерархичной модели по сравнению с существующими – сетевой и шунтированной, является наиболее простой, упорядоченный и систематизированный процесс проверки клиентом одного ЦСК сертификата клиента другого ЦСК. Очевидным недостатком этой архитектуры является то, что в случае нарушения работы корневого центра сертификации ключей практически нарушается работа всей системы в целом. То есть, если будет скомпрометирован секретный ключ корневого ЦСК, все сертификаты, которые были сформированы им центрам сертификации ключей, будут также скомпрометированы и должны быть заменены.

Поэтому, проектирование корневого ЦСК и последующее выполнение им своих функциональных обязанностей основывается на выполнении более строгих организационно-технических требований по обеспечению безопасности информации, чем предъявляются к другим субъектам, например, к центрам сертификации. От надежности защиты этого центра и доверия к нему в большой степени зависит надежность всей системы в целом.

Итак, как уже отмечалось, НИОК в соответствии с законопроектом “Об электронной цифровой подписи” строится по иерархической архитектуре.

В повседневной практике это двухуровневая схема: центральный удостоверяющий орган (корневой ЦСК) ---- центры сертификации ключей (подчиненный ЦСК), а в случае использования технологии ЭЦП в государственных органах предусматривается возможность использования трехуровневой системы сертификации: центральный удостоверяющий орган ---- удостоверяющие центры ----- центры сертификации ключей. Кроме этого, не предусматривается возможность перекрестной сертификации между центрами сертификации ключей (кросс-сертификация). Это сделано, прежде всего, для четкого регламентирования процесса приравнивания ЭЦП к собственноручной подписи, а также обеспечения достаточного уровня доверия к сертификатам открытых ключей между пользователями. Ключи конечных пользователей могут

генерироваться как ими самими, так и центром сертификации ключей. Вместе с тем, ознакомление и хранение секретных ключей конечных пользователей в центре сертификации не допускается.

В НИОК корневым центром для всех ЦСК, удостоверяющих центров и конечных пользователей является центральный удостоверяющий орган (ЦУО), который является центром сертификации первого уровня.

Основными задачами ЦУО являются регистрация центров сертификации второго уровня, т. е. ЦСК и удостоверяющих центров, формирование и публикация в сетевом справочнике их сертификатов. Кроме этих функций ему также предоставляются полномочия по выполнению функции технического управления, руководства и контроля над механизмом функционирования системы ЭЦП.

Кроме этого, ЦУО, вероятно, будет выполнять функции, связанные с обеспечением технической возможности признания иностранных сертификатов.

В соответствии с законопроектом иностранные сертификаты ключей, выданные центрами сертификации ключей, расположенными за границей, признаются в соответствии с нормами и принципами международного права. Технически признание иностранных сертификатов, очевидно, будет достигаться путем взаимной сертификации (кросс-сертификации) центрального удостоверяющего органа с аналогичными корневыми центрами сертификации ключей иностранных государств.

Центрами сертификации второго уровня являются удостоверяющие центры (аналог центрального удостоверяющего органа, действия которого ограничены конкретным государственным органом, например, удостоверяющий центр Министерства обороны Украины или удостоверяющий центр Национального банка Украины), а также центры сертификации ключей, сертификат которым сформировал непосредственно ЦУО. Удостоверяющие центры регистрируются и получают сертификаты в ЦУО.

Удостоверяющие центры регистрируют подчиненные центры сертификации третьего уровня, формируют и публикуют в сетевом справочнике их сертификаты, а также список отозванных сертификатов ЦСК. Удостоверяющие центры не предоставляют услуг цифровой подписи конечным пользователям.

ЦСК могут быть аккредитованными или не аккредитованными. Аккредитованные ЦСК – те, которые прошли определенную процедуру аккредитации и отвечают специальным требованиям. К не аккредитованным ЦСК, согласно законопроекту, не предъявляется практически никаких требований, кроме необходимости получения сертификата в ЦУО.

ЦСК формируют свои секретные и открытые ключи, регистрируются в вышестоящем центре (ЦУО или удостоверяющем центре) и получают у них сертификаты.

Главной задачей центров сертификации является формирование сертификатов конечных пользователей на основе данных, полученных от подчиненных центров регистрации.

Центры регистрации обеспечивают организационно-технические мероприятия, связанные с регистрацией и подтверждением идентичности конечных пользователей в системе. В задачи ЦР может также входить публикация сертификатов и списка отозванных сертификатов (СОС), сформированных ЦС, в сетевом справочнике.

С учетом необходимости обеспечения потребностей в механизмах ЭЦП органов государственной власти и других юридических и физических лиц, НИОК должна поддерживать две подсистемы. Первая подсистема – для обеспечения потребностей в услугах ЭЦП органов государственной власти, органов местного самоуправления, предприятий, учреждений и организаций государственной формы собственности. Иерархический принцип построения государственного управления подразумевает и соответствующую структуру построения в перспективе системы центров сертификации ключей для электронного оборота: от уровня высших органов власти (Верховной Рады, Кабинета Министров, Администрации Президента), до центральных органов исполнительной власти, местных органов самоуправления и отдельных организаций.

В этой подсистеме порядок предоставления услуг и особенности использования цифровой подписи органами государственной власти устанавливаются Кабинетом Министров Украины.

Вторая подсистема – для обеспечения потребностей других юридических и физических лиц, построение и развитие которой планируется за счет всевозможных внебюджетных инвестиций и вложений.

При этом пользователи обеих подсистем имеют возможность взаимодействия и для них этот процесс должен быть абсолютно прозрачен.

Весь спектр вопросов информационной безопасности, возникающих при построении и обслуживании НИОК, можно разделить на следующие разделы:

вопросы сетевой безопасности (для компонентов НИОК, подключенных к общедоступным каналам передачи данных);

вопросы защиты от несанкционированного доступа;

требования к криптографической компоненте центров сертификации.

Обеспечение безопасности при использовании сертификатов открытых ключей складывается как из обеспечения безопасного функционирования аппаратно-программной платформы, на которой

функционируют центры сертификации, так и из обеспечения безопасности непосредственно самих сертификатов.

Практически все прикладные сферы (электронный документооборот, электронная коммерция и т. д.), цифровая подпись для которых является одним из основных компонентов, становятся все более глобальными и интегрированными. Поэтому вопрос совместимости, в том числе механизмов ЭЦП, становится все более актуальным.

Очевидно, что отсутствие согласованного формата сертификата может привести к неоднозначному толкованию его полей теми ЦСК, которые их формируют, и приложениями, которые их используют. Как следствие, неверная интерпретация содержимого полей сертификата может спровоцировать приложение на использование сертификата не по назначению или, наоборот, приведет к неправомочному отказу в предоставлении определенной услуги пользователю данного сертификата.

Приведенный пример иллюстрирует проблему, которую можно обозначить как проблему совместимости криптографических приложений на уровне ИОК: параметры сертификатов, ЦСК для поддержания определенной ИОК системы должны правильно "пониматься" и однозначно интерпретироваться любым приложением (независимо от его производителя), пользующимся услугами указанного ЦСК. Эта проблема достаточно легко разрешается при условии, что все ЦСК НИОК будут придерживаться единой структуры и формата представления данных в составе сертификата.

Данный момент представляется достаточно важным, так как единый стандарт на сертификаты является краеугольным камнем в построении иерархической структуры ЦСК и унификации подсистем распределения криптографических ключей в различных приложениях.

Содержащиеся в законопроекте требования к условиям использования ЭЦП, процедурам сертификации открытых ключей, обязательствам ЦСК и владельцев сертификатов и пр. по существу соответствуют описанию системы ИОК (PKI), определенной международным стандартом X.509, хотя явно этот стандарт в законе и не упоминается.

Естественно, что для приведения формата сертификата X.509 в соответствие с положениями Закона “Об электронной цифровой подписи” потребуются некоторые согласования по составу отдельных полей и атрибутов сертификата, однако возможность реализации требований закона легко обеспечивается гибкостью стандарта X.509.

К сожалению, введение единого стандарта на сертификаты само по себе еще не решает проблемы унификации ИОК, поддерживающей разные средства цифровой подписи в единой НИОК. К примеру, в данное время даже сертифицированные средства криптографической защиты информации (КЗИ) различных производителей, реализующие криптографические стандарты, принятые в Украине, практически несовместимы между собой. Как правило, каждое средство КЗИ использует свои собственные идентификаторы алгоритмов, форматы представления их параметров и форматы хранения ключевой информации.

Может возникнуть ситуация, когда сертификаты, сформированные ЦСК, поддерживающими разные средства цифровой подписи различных украинских производителей, окажутся несовместимы между собой, даже если они придерживаются единого формата сертификата и реализуют один и тот же криптографический стандарт ЭЦП. Соответственно, цифровая подпись, сформированная одним средством ЭЦП, не может быть проверена другим средством.

Таким образом, без собственных идентификаторов алгоритмов, единых форматов представления их параметров, форматов хранения ключевой информации приложения различных производителей могут взаимодействовать друг с другом, если используют зарубежные криптографические алгоритмы (например, RSA, DSA), для которых созданы и зарегистрированы описанные атрибуты. Для решения проблем совместимости необходимо провести работу по присвоению унифицированных идентификаторов национальным объектам.

Любой разработчик по номеру идентификатора может получить всю необходимую информацию о параметрах алгоритма, самом алгоритме, форматах, протоколах и пр.

Сейчас в Украине, в связи с введением нового государственного стандарта на ЭЦП (ДСТУ 4145-2002), сложился крайне благоприятный момент для принятия единого стандарта на формат представления параметров алгоритма ЭЦП и приведения в соответствие с международными стандартами структуры и форматов представления данных в составе сертификата (включая формат представления открытого ключа и ЭЦП).

Кроме этого, подобная стандартизация необходима для обеспечения прозрачности исполнения требований норм закона об ЭЦП независимо от используемых средств электронной подписи. Совместимость средств ЭЦП на уровне НИОК дает два важных преимущества:

- приложения любых украинских производителей смогут использовать сертификаты любых ЦСК, удовлетворяющих требованиям закона об ЭЦП;
- электронная подпись, выполненная приложением одного производителя, может быть проверена приложением другого.

Также в НИОК должна быть определена общая политика сертификации, которая представляет собой правила использования сертификатов и сертификационных услуг, а также правила поведения в случае наступления того или иного события. К примеру, если пользователь по ошибке отослал получателю секретный ключ, то в соответствии с правилами ему может быть предписано сообщить об этом ЦСК сообщением о компрометации секретного ключа.

Таким образом, в процессе проектирования национальной системы электронной цифровой подписи должны быть решены следующие вопросы.

1. Разработан порядок и протоколы взаимодействия между субъектами системы ЭЦП, в частности процедуры получения или отзыв сертификата конечного пользователя, ЦСК, центральный удостоверяющий орган.

2. Разработана типовая политика сертификации в НИОК (типовой регламент функционирования ЦСК) – формализованный документ, определяющий порядок взаимодействия ЦСК с владельцами сертификатов, а также с другими ЦСК, обязанности и ответственность участников документооборота, принципы осуществления физической и технической защиты, идентификация и аутентификация субъектов информационного взаимодействия и т. д. Данный документ должен учитывать особенности использования цифровой подписи для разных категорий пользователей, возможные сферы применения механизмов цифровой подписи и т. д.

3. Разработан национальный профайл сертификата (формат) и списка отозванных сертификатов. Указанный документ должен определить и описывать расширения (основные и дополнительные поля), которые используются при формировании сертификатов, стандартизировать форматы представления ключей, хранящихся на ключевых носителях и в составе сертификата, а также унифицировать значения и форматы представления параметров алгоритма ЭЦП.

4. Разработка и правовая регистрация национальной иерархии объектных идентификаторов для специфических дополнений, криптографических алгоритмов, их параметров и т. д.

В заключение хотелось бы отметить, что процесс создания систем ЦСК для защищенного документооборота в масштабах такого государства, как Украина, займет весьма продолжительное время и потребует привлечения значительных финансовых и других ресурсов. Поэтому поэтапное и параллельное создание описанных подсистем общей системы НИОК позволит, с одной стороны, сэкономить ресурсы, с другой стороны – относительно быстро включить в электронный документооборот системы органов государственного управления Украины с отдельными юридическими и физическими лицами.

УДК 62.001.4

ОРГАНИЗАЦИЯ МЕЖЛАБОРАТОРНЫХ ИСПЫТАНИЙ

Евгений Володарский, Игорь Харченко*

Национальный технический университет Украины "КПИ"

**Украинский НИИ пожарной безопасности*

Анотація: **Розглядаються особливості організації міжлабораторних випробувань на перевірку повторюємості та відтворюємості результатів, що дозволяє враховувати не тільки вплив випадкових фікторів, але й індивідуальні властивості лабораторій.**

Summary: **It is considered the properties of organization interlaboratory tests on repeatability and reproducibility checriny. It allows to tare into account not only influence of the random factors but specific laboratory property.**

Ключові слова: **Испытания, повторяемость, воспроизводимость.**

I Введение

В соответствии с [1] испытания заключаются в экспериментальном определении количественных и (или) качественных характеристик свойств объекта как результата воздействия на него при его функционировании. Характерной чертой испытаний является проведение экспериментальных исследований при нормированных условиях, которые задаются в нормативной документации. Таким образом, существенным отличием между