УДК 004.056: 004.414.3: 004.057.2

Сергей Васильевич Мартыненко, Юрий Юрьевич Андреев

ТРЕБОВАНИЯ НАДЕЖНОСТИ СРЕДСТВ СОЗДАНИЯ ЭЦП

Аннотация: В статье проведен анализ требований надежности (безопасности) программно-аппаратных средств создания электронной цифровой подписи (ЭЦП), изложенных в международных стандартах. В терминах стандарта FIPS 140-2 разработан перечень минимальных требований к Аппаратным Модулям Безопасности (HSM), применяемых в приложениях Центра сертификации ключей и пользовательских серверных приложениях.

Применение электронной цифровой подписи (ЭЦП) обусловлено широким развитием электронной техники и постепенного перехода от бумажного документооборота к электронному.

В нашем государстве использование электронной подписи для подписи документов в электронном виде приравнивается к обычной подписи, согласно закону про ЭЦП [1]. ЭЦП создается при помощи программно-аппаратных средств, которые должны отвечать требованиям *надежности* таких устройств.

Согласно законодательству Украины «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.» [1]. Однако при разработке и создании надежных устройств создания ЭЦП требуются четкие критерии, основанные на стандартах. При этом следует учитывать соответствующие требования и стандарты Европейского Сообщества (ЕС), на интеграцию с которым взяла курс Украина. Рассмотрим эти вопросы.

Требования, предъявляемые к надежным средствам создания ЭЦП для нашей страны и принятые в мировой и европейской практике различны. В частности, Директива ЕС [2] предъявляет такие минимальные требования к надежным/безопасным механизмам создания подписи (secure signature-creation devices):

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.

В целом, требования надежности программно-аппаратных средств ЭЦП можно подразделить на следующие категории:

- требования к программному обеспечению и среде исполнения;
- требования к аппаратному обеспечению.

Проанализировав документы [1]–[9] можно сделать выводы, что наиболее полный набор требований предоставлен в документе [5].

Рассмотрим документ NIST FIPS 140-2 [5], определяющего требования, которым должны удовлетворять криптографические модули, используемые в системах защиты информации.

Этот стандарт описывает 4 уровня безопасности, первый из которых имеет минимальные требования, четвертый, на настоящее время, максимальные требования безопасности. Эти требования безопасности относятся к областям, связанным с разработкой и применением криптографических модулей. Они включают описание криптографических модулей, их порты и интерфейсы, роли, обслуживание и аутентификацию, модель конечных состояний, защиту от внешних воздействий, среду использования, управление криптографическими ключами, электромагнитные излучения, самотестирование, точность изготовления и максимальную защищенность от атак.

Уровень 1 описывает минимальные требования безопасности без требований к аппаратному устройству. В качестве примера приводится компьютерная плата, предназначенная для шифрования [5]. Этот уровень позволяет использовать программные или аппаратные компоненты без требований к операционной системе и среде выполнения. Такие системы предназначены для построения недорогих решений по защите информации защите сетевого трафика и т.д.

Уровень 2 дополняет уровень 1 требованиями к физической защите устройств шифрования. Эти требования включают наличие специальных покрытий, замков и других средств, ограничивающих доступ к шифрующему устройству и средств, не позволяющих скрытный физический доступ к устройству шифрования. Этот уровень требует как минимум основанную на роли идентификацию оператора, который имеет право вносить изменения в параметры криптомодуля. Кроме того, программные модули должны исполняться в операционной системе, которая:

- удовлетворяет функциональным техническим условиям, определенным в Common Criteria (CC) Protection Profiles (PPs);
- отвечает общим требованиям уровня гарантии EAL2 (Evaluation Assurance Level) или больше.

Уровень 3 расширяет требования уровня 2 к физическим устройствам тем, что защищенные модули должны иметь дополнительные цепи, сообщающие

устройству о попытке доступа к нему, при котором криптопровайдер и/или устройство полностью удаляет все секретные данные и настройки. Этот уровень расширяет дополнительные требования по идентификации оператора, обслуживающего устройство, подтверждением подлинности и наличие разрешения идентифицированному оператору на определенные действия с модулем. Кроме того, этот уровень требует физического разделения входных и выходных потоков данных. Этот уровень предполагает использование операционной системы для программных компонентов и библиотек, которая:

- удовлетворяет функциональным техническим условиям, определенным в Common Criteria (CC) Protection Profiles (PPs) с дополнительными функциональными требованиями Trusted Path (FTP_TRP.1); и
- отвечает общим требованиям уровня гарантии EAL3 или выше с дополнительными гарантиями Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1).

Уровень 4 обеспечивает максимальные требования к физическим устройствам для данного стандарта и предполагает использование оболочки, предотвращающей любую неавторизированную попытку физического доступа. При обнаружении любой попытки доступа в устройстве и/или криптопровайдере немедленно обнуляются все секретные данные и ключевая информация. Кроме того, такое устройство должно иметь защиту от воздействий окружающей среды (температурные или электрические колебания, и другое), так как такие воздействия могут быть результатом атаки с целью нарушить работоспособность криптомодуля. Этот уровень предполагает использование операционной системы для программных компонентов и библиотек, которая:

- удовлетворяет функциональным техническим условиям, определенным для Уровня Безопасности 3; и
- отвечает общим требованиям уровня гарантии EAL4 или выше.

Требования безопасности, предъявляемые соответственно уровням 1-4 приведены в табл.1.

Таблица 1.

	Уровень 1	Уровень 2	Уровень 3	Уровень 4
Спецификация криптографических модулей	Спецификация криптографических модулей, криптографические ограничения, сертифицированные алгоритмы и сертифицированные параметры их работы. Описание криптографических модулей включая аппаратные, программные и встроенные компоненты. Описанная политика безопасности.			

	Уровень 1	Уровень 2	Уровень 3	Уровень 4
Порты и интерфейсы криптомодулей	Требуемые и дополнительные интерфейсы. Спецификация всех интерфейсов и всех потоков.		Потоки данных с незащищенной информацией должны быть логически отделены.	
Роли, сервисы и определение достоверности	Логическое разделение необходимых и дополнительных ролей и услуг.	Установление подлинности оператора на основе идентичности или на основе роли.	Установление подлинности оператора на основе идентичности.	
Модель конечных состояний	Описание модели конечных состояний. Требуемые состояния и необязательные состояния. Диаграмма переходов и описание условий перехода.			
Безопасность устройства	Класс промышленного оборудования	Замки или специальные пломбы	Пломбы и реакция на физический доступ	Обнаруже-ние доступа и удаление ключевой информации, Защита от изменения окружающей среды
Среда эксплуатации	Один оператор. Исполняемый код. Сертифицированное устройство.	Описывается политикой безопасности соответствующей EAL2 или выше с соответствующим уровнем доступа и аудита	Описывается политикой безопасности соответствующей EAL3 или выше с моделированием политики безопасности	Описывается политикой безопасности соответствующей EAL4 или выше
Управление криптографическими ключами	Управление ключами: генератор случайных чисел и ключей, импортирование ключей, распространений ключей, хранилище ключей и уничтожение (обнуление) ключей.			

	Уровень 1	Уровень 2	Уровень 3	Уровень 4
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Самотести рование	Тесты при подаче питания: тест криптографических алгоритмов, совместимость программных и встроенных модулей, тесты критических функций. Тесты общего состояния.			
Точность реализа-ции	Управление конфигура-цией, Безопасная установка и настройка. соответствие реализации настройкам безопасности. Руководства по эксплуатации	Управление конфигура-цией. Безопасное распространение. Функциональная специфика-ция.	Исполнение на языке высокого уровня	Формальная модель. Детальные описания (неформаль-ные доказа-тельства). Предвари-тельные состояния и оконча-тельные состояния
Минимиза ция других воздей-ствий	Спецификация уменьшения воздействий, для которых никакие тестируемые требования не являются в настоящее время доступными.			

Исходя из перечисленных выше требований, можно сделать вывод, что надежные устройства ЭЦП должны соответствовать уровням безопасности 2, 3 или 4. Однако необходимо отметить, что это требования безопасности, предъявляемые к криптографическим устройствам. Такие модули, в частности, содержат и функциональность (криптоалгоритмы) ЭЦП. Более детальные требования, предъявляемые именно к устройствам ЭЦП, приводятся в документе [8]-[9].

Кроме того, сама ключевая информация должна находиться под контролем согласно правил безопасности для соответствующих государственных органов, иначе говоря, такая информация не должна покидать устройства шифрования, используемого для создания ЭЦП.

На основании вышеуказанных документов можно сделать вывод, что на настоящее время к безопасным устройствам создания ЭЦП можно отнести

программно-аппаратные средства, отвечающие уровням 2, 3 или 4 по FIPS PUB 140-2 [5] и отвечающим требованиям приложения 3 документа [1].

Основываясь на вышеизложенном, ниже предлагается спецификация требований, как обязательных, минимальных требований для совместимости, работы и безопасности надежных/безопасных программно-аппаратных механизмов создания ЭЦП:

1. *Область применения*. *Подписант* (физическое лицо/индивидуум или автоматизированная система/компьютер) может генерировать ЭЦП, используя любой из методов:

- Интеллектуальную карточку (смарт-карту) или другое персональное средство аутентификации (токен - token), которые удовлетворяют требования персональной ответственности за любые генерируемые подписи, или
- Аппаратный Модуль Безопасности (HSM - Hardware Security Module), удовлетворяющий требованиям, сформулированным ниже. Модуль HSM применяется там, где требуется автоматизированный процесс подписывания.

На практике, Подписант может объединить автоматизированные и ручные операции и поэтому использовать как интеллектуальные карточки, так и HSM. Например, транзакционные сообщения, исходящие от Подписанта (т.е. как подпись Клиента/Заказчика), могут подписываться, используя интеллектуальную карточку под управлением индивидуума. Однако запросы о статусе или подтверждении (проверки) подписей могут генерироваться автоматически сервером, использующим встроенный HSM и управляемый как ресурс системы.

2. *Множественность ключей HSM*. Модули HSM быть способны поддерживать все обязательные ключи. Там где это возможно, один ключ должен применяться для одной цели. Реализации HSM должны позволять также использовать сеть HSM, чтобы поддерживать все обязательные ключи.

3. *Выбор ключа без переконфигурирования*. В настоящее время, нет никаких требований совместимости. Однако так как большинство участников будет требовать от HSM, чтобы они поддерживали более одного ключа подписи, то *активный ключ* подписи, который означает ключ, который загружен в HSM для использования (например, ключи для SSL, OCSP-ответчика, OCSP-запросчика и т.п.), должен использоваться без переконфигурирования HSM.

4. *Использование для инициализации и персонализации смарт-карт*.

Если HSM применяется для *инициализации и персонализации смарт-карт,* должны выполняться, как минимум, требования:

• Учет числа персонализированных смарт-карт. Хранимое в HSM внутреннее значение, увеличивается на единицу каждый раз, когда генерируется ключевая пара для персонализации смарт-карт.

• Генерация ключевых пар для инициации и персонализации интеллектуальных карточек может осуществляться с использованием устройства HSM в безопасном окружении. При этом должна быть относительная гарантия того, что ключевая пара генерируется и записывается на смарт-карту так, что в любое время существует только один образец приватного ключа и что после записи его на карту, ключ в HSM уничтожается.

5. *Требования уровня безопасности.* Модули HSM, используемые для разных приложений, могут соответствовать разным уровням безопасности. В таблице 2 конкретизируется функциональная область, где используется HSM, и указываются обязательные минимальные требования (уровень) безопасности.

Допускаются такие исключения из правил, приведенных в табл.2:

1) Может эксплуатироваться HSM, который был однажды сертифицирован, но этот сертификат стал недействительным из-за обновления продукта, которое обладает большим или равным уровнем безопасности.

2) HSM, который не был никогда сертифицирован и не имеет никакого сертификата, не может использоваться.

3) HSM, который в настоящий момент находится на сертификации, может использоваться в течение временного периода сертификации.

Заметим, что в таблице 2 ниже, в колонках HSM приведены данные для SSL Web-сервера. Эти же данные применяются и к другим серверам пользователей.

Таблица 2. Уровень безопасности HSM от функции

	Функциональная область	Минимальная поддерживаемая длина ключа (RSA)	Генератор случайных чисел HSM	Уровень сертификации HSM
ЦСК	CA	2048	FIPS 140-2 Уровень 3	FIPS 140-2 Уровень 3
	OCSP Responder	1024	FIPS 140-2 Уровень 3	
	Смарт-карт персонализация	1024	FIPS 140-2 Уровень 3	
	RA	1024	FIPS 140-2 Уровень 3	FIPS 140-2 Уровень 2

Пользователи**	Функциональная область	Минимальная поддерживаемая длина ключа (RSA)	Генератор случайных чисел HSM	Уровень сертификации HSM
	DSMS*	1024	FIPS 140-2 Уровень 3	FIPS 140-2 Уровень 2
	Web-сервер SSL	1024	FIPS 140-2 Уровень 3	FIPS 140-2 Уровень 2

*системы подписи сообщений (Digital Signature Messaging System, DSMS)

** банки, коммерческие организации, физические лица.

Для формирования требований безопасности к HSM можно использовать вместо FIPS 140-2 равноценный Госстандарт.

Кроме требований относительно подписи, приведенных выше, к HSM также должны выдвигаться требования относительно шифрования. Спецификация этих требований зависит от устройства и целей/функций, им выполняемых. Однако минимальные требования должны включать:

- Должен использоваться алгоритм и ключ шифрования, эквивалентные, как минимум, двух-ключевому 3DES (two-key triple-DES);
- Если данные экспортируются в формате открытого текста (plaintext), то их необходимо разделить, как минимум, на две компоненты.

Если HSM хранит приватный/секретный ключ на внешней карте/модуле, то должны выполняться следующие минимальные требования безопасности:

- Приватный/секретный ключ должен храниться в зашифрованном файле, защищенном, как минимум, 128-разрядным шифрованием 3DES;
- Каталог/директория, где размещен приватный/секретный ключ, не должен открываться для общего доступа;
- Ключ должен расшифровываться только в пределах непосредственно HSM;
- При начальной установке HSM нужно сконфигурировать так, чтобы требовать участия минимум двух лиц для целей запуска/обновления;
- Распространяемые электронным способом секретные и приватные ключи должны вводиться и выводиться, как минимум, формате эквивалентном 3DES-шифрованию.

Таким образом, выше предложен в терминах стандарта FIPS 140-2 перечень минимальных требований к аппаратным модулям безопасности HSM, применяемых в приложениях Центра сертификации ключей и пользовательских серверных приложениях, что позволит разработчикам различных программно-аппаратных автоматизированных комплексов и обслуживающему персоналу этих комплексов иметь минимальную шкалу требований безопасности. Кроме того, термин «сертификат соответствия»,

который используется для определения надежных средств ЭЦП [1], означает, что устройство соответствует некоторому стандарту или четко выписанным требованиям, а не техническому заданию на разработку этого устройства.

Конечно, предложенные выше требования должны быть обсуждены рядом специалистов и утверждены в качестве нормативных в установленном порядке.

Литература

1. Закон України про електронний цифровий підпис № 852–IV від 22 травня 2003 року.
2. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures).
3. Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1451 «Положення про центральний засвідчувальний орган».
4. Постанова Кабінету Міністрів України від 13 липня 2004 р. №903 «Про затвердження Порядку акредитації центру сертифікації ключів».
5. FIPS PUB 140-2 Federal information processing standards publication (Supercedes FIPS PUB 140-1, 1994 January 11).
6. FIPS PUB 140-1: Federal information processing standards publication - 1994 January 11.
7. Annabelle Lee. Guideline for Implementing Cryptography in the Federal Government. - NIST Special Publication 800-21, November 1999.
8. CWA 14169. Secure signature-creation devices “EAL 4+” - EUROPEAN COMMITTEE FOR STANDARDIZATION, Ref. No.:CWA 14169:2004 E, March 2004.
9. CWA 14170. Security requirements for signature creation applications - EUROPEAN COMMITTEE FOR STANDARDIZATION, Ref. No.:CWA 14170:2004 E, May 2004.