УДК 004.05

АРМ СЭП КС3 на базе компьютера с "гарвардской" архитектурой

Д. Ю. Счастный
ЗАО «ОКБ САПР», Москва, Россия

Предложен подход к реализации экономичного АРМ СЭП класса КС3, в основе которого применение вместо архитектуры x86 компьютера с "гарвардской" архитектурой.

Ключевые слова: "гарвардская" архитектура, СЭП, среда функционирования криптографии.

Весной 2011 г. в Федеральном Законе №63-ФЗ «Об электронной подписи» было введено понятие «средства электронной подписи» (СЭП). В тексте Закона СЭП определяется как «шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций — создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи». Там же описан и основной функционал СЭП. Они должны: 1) позволять устанавливать факт изменения подписанного электронного документа после момента его подписания; 2) обеспечивать практическую невозможность вычисления ключа электронной подписи (ЭП) из ЭП или из ключа ее проверки.

Также при создании электронной подписи СЭП должны:

– показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

– создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;

– однозначно показывать, что ЭП создана.

А при проверке электронной подписи СЭП должны:

– показывать содержание электронного документа, подписанного ЭП;

– показывать информацию о внесении изменений в подписанный ЭП электронный документ;

– указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Описанные выше требования к СЭП при создании и проверке ЭП не относятся к СЭП, используемым для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Счастный Дмитрий Юрьевич, зам. генерального директора.
E-mail: DimaS@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

В конце 2011 г. вышел приказ ФСБ №796, в котором вводятся классы СЭП и детализируются требования к ним. Важным понятием, на котором делается акцент в этом документе, является среда функционирования (СФ) СЭП. И к СФ СЭП, наряду с самим СЭП, предъявляются требования, т. е. документ не рассматривает СЭП изолировано от технологических процессов обработки информации, а взаимоувязывает его со средой, в которой оно выполняет свои штатные функции. И важно, что СФ упоминается в контексте требований о необходимости визуализировать документ перед его подписанием или проверкой подписи (дословно повторяющих соответствующие требования ФЗ-63). Иными словами, регулятор включает в зону своей ответственности подтверждение (сертификатом соответствия СЭП своим требованиям) невозможности ситуации, когда человек видит одни данные, а подписывает совершенно другие.

Таким образом, СЭП это не только СКЗИ, способное работать с ключами и сертификатами ЭП, но и СФ (совокупность программных и аппаратных средств), в которой пользователь работает с документами и в которой выполняются криптографические операции. В данном ракурсе традиционные подходы к работе с ЭП на компьютерах x86-архитектуры под управлением ОС Windows приводят к необходимости существенного удорожания решений (к стоимости собственно СКЗИ добавляется стоимость средств защиты информации для обеспечения корректной СФ) либо к использованию СЭП низших классов (без значительных затрат создать СЭП класса выше КС2 представляется затруднительным).

В качестве примера альтернативы приведем реализацию СЭП класса КС3 на базе компьютера с "гарвардской" архитектурой.

Данное решение базируется на аппаратной платформе Aquarius CMP TCC S60-10. В качестве операционной системы используется клон Linux (aQuaSEPStd). Криптосистема состоит из трех частей:

- ключевого хранилища (ПСКЗИ ШИПКА-лайт Slim), совмещенного с аппаратным идентификатором пользователя;

- аппаратного криптоядра (ПСКЗИ ШИПКА);
- библиотеки электронной подписи (БЭП).

В ключевом хранилище в зашифрованном виде хранится ключ ЭП пользователя и соответствующий ему сертификат ключа проверки ЭП. Сертификат хранится в открытом виде. Аппаратное криптоядро (ШИПКА) находится стационарно внутри АРМа, причем установлено оно в стационарный USB-разъем, развернутый внутрь АРМа. БЭП выполнено в виде специального программного обеспечения, позволяющего из стороннего приложения вызывать функции аппаратного криптоядра. В качестве визуализатора документов при подписании документов используется браузер Mozilla, и в него же встраивается БЭП для подписания документов формата XML произвольной длины.

Особенностью решения является работа операционной системы в режиме «только чтение». Причем этот режим обеспечивается аппаратно путем перевода микросхемы памяти в состояние запрета записи. Эта особенность (невозможность записи на диск) позволяет жестко раз и навсегда обеспечить неизменность СФ СЭП, правда, приводит к невозможности ведения журналов работы СЭП на этом жестком диске. По этой причине для хранения журналов используется память ШИПКИ, стационарно установленной в АРМ. Ее объем (до 1 мегабайта) позволяет хранить журналы работы СЭП продолжительное время.

Типичный сценарий работы пользователя на таком АРМ выглядит следующим образом.

1. На специальном АРМе создается ключ ЭП, соответствующий ему ключ проверки ЭП, и формируется запрос на выпуск сертификат ключа проверки ЭП.

2. Ключ ЭП в зашифрованном виде сохраняется на ключевой носитель пользователя, а запрос на выпуск сертификат отправляется в УЦ.

3. После соответствующей обработки УЦ возвращает сертификат ключа проверки ЭП, и он записывается на ключевой носитель.

4. После этого администратор записывает на этот же ключевой носитель признаки принадлежности именно этой автоматизированной системе, и пользователь получает возможность работать на любом АРМ системы.

5. При подключении ключевого носителя к АРМу модуль контроля входа в систему проверяет наличие признака принадлежности системе в предъявленном ключевом носителе и запрашивает пин-код, на основании которого открывается доступ к зашифрованному ключу ЭП пользователя.

6. После этого ключ ЭП в зашифрованном виде копируется в аппаратное криптоядро.

7. Пользователь запускает браузер, подключается к серверу информационной системы и начинает работать с документами.

8. Когда необходимо подписать документ, пользователь нажимает кнопку «Подписать» на web-форме, документ передается на АРМ, визуализируется, от него с помощью БЭП аппаратное криптоядро вычисляет значение хеш-функции и вырабатывает ЭП на ключе пользователя.

9. Пользователь информируется о факте выработки ЭП, и документ возвращается на сервер вместе с созданной ЭП.

10. После завершения работы пользователя ключи уничтожаются внутри аппаратного криптоядра.

В случае нештатного завершения работы АРМ ключи будут уничтожены при последующем включении АРМ или при подключении криптоядра к другому АРМ.

Все операции, производимые на АРМ (вход пользователя, завершение работы, создание ЭП), записываются в энергонезависимую память криптоядра.

Предложенное решение АРМ СЭП КС3 стоит недорого, выполняет все требования к СЭП класса КС3 и может достаточно легко встраиваться в различные автоматизированные системы обработки данных.

Electronic signature tool WKS KC3 class realization on the "Harvard" architecture based computer

D. Yu. Schastny
OKB SAPR JSC, Moscow, Russia

The article is offering the approach to the efficient realization of electronic signature tool WKS by using "Harvard" architecture based computer.

Keywords: "Harvard" architecture, electronic signature tool, cryptography operating environment.

Received June 14, 2014