И. С. Мурзенков, В. М. Ничипорчук

РАЗРАБОТКА МЕХАНИЗМА ОБЕСПЕЧЕНИЯ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ ДЛЯ АВТОРИЗАЦИИ ИНТЕРНЕТ-ПЛАТЕЖЕЙ

Современные банковские технологии составляют основу электронной коммерции. Во всех подсистемах банки используют такие электронные технологии, как системы управления базами данных, средства электронной подписи (ЭП), средства идентификации и аутентификации, основанные на системах и протоколах защищенной связи. Благодаря развитию технологий, связанных с Интернетом, некоторые банки, занимающиеся обслуживанием предприятий электронной коммерции и физических лиц, потребляющих услуги электронной коммерции (в первую очередь коммуникационные услуги сервис-провайдеров и операторов мобильной связи), начали внедрять модель дистанционного обслуживания [1]. В основе этой модели лежит использование стандартных средств связи, например коммутируемых телефонных линий, стандартных транспортных протоколов, стандартных средств шифрования данных и средств ЭП, а также стандартных средств вычислительной техники — персональных компьютеров. В связи с этим возникла необходимость использования средств квалифицированной электронной подписи в моделях дистанционного обслуживания банков и авторизации интернет-платежей.

На сегодняшний день для использования различных систем дистанционного обслуживания необходимо устанавливать или настраивать различное дополнительное программное обеспечение. Использование квалифицированной ЭП в браузере позволило бы создавать такие системы без дополнительного программного обеспечения и выполнять все функции, применяя только веб-технологии.

В соответствии с действующим российским законодательством [2], видами ЭП являются простая и усиленная ЭП. Формат подписи изображен на рис. 1. Различаются усиленная неквалифицированная и усиленная квалифицированная ЭП.

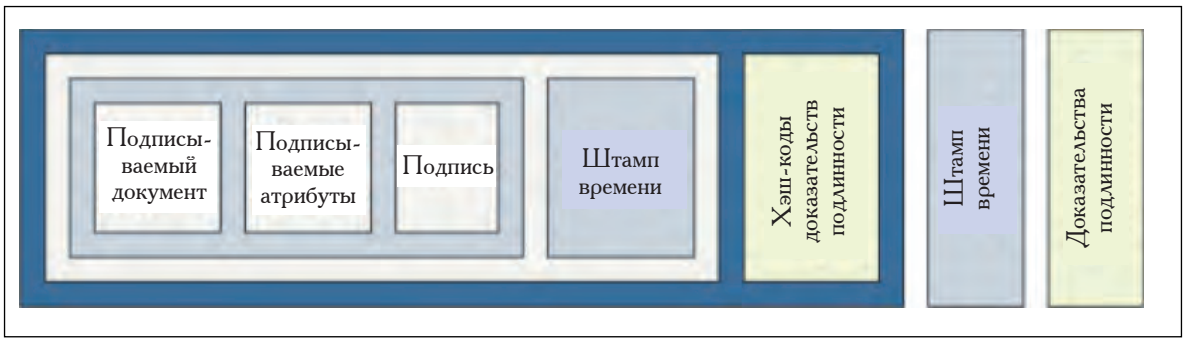

Рис. 1. Формат усовершенствованной электронной подписи

Простой ЭП является такая электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной ЭП является такая электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Квалифицированной ЭП является такая электронная подпись, которая соответствует всем признакам неквалифицированной ЭП и следующим дополнительным признакам:
- ключ проверки ЭП указан в квалифицированном сертификате;
- для создания и проверки ЭП используются средства ЭП, получившие подтверждение соответствия требованиям.

Программно-аппаратная часть для обеспечения усиленной ЭП представляет собой виртуальную машину с установленной операционной системой Microsoft Windows 7 Professional x86.

В качестве рабочей среды используется веб-форма, содержимое которой предназначено для подписи. В функциональные возможности системы входят:
- создание электронной подписи;
- проверка электронной подписи.

Система функционирует в любом из современных браузеров с поддержкой сценариев JavaScript:
- Internet Explorer;
- Opera;
- Chrome;
- Safari;
- Mozilla Firefox.

Создание и проверка подписи происходят на стороне клиента. При создании подписи она добавляется к подписываемым данным.

В веб-приложениях по умолчанию доступен объектно-ориентированный скриптовый язык программирования JavaScript. Так как JavaScript не может напрямую вызывать функции криптопровайдера, необходимо использование специального компонента (плагина) для взаимодействия с криптопровайдером. Плагин взаимодействует с Javascript-программой в обе стороны. Он позволяет уведомлять Javascript-программу о различных событиях, таких как успешная инициализация плагина или отмена решения о подписи содержимого.

Для создания и проверки электронной подписи на веб-страницах установлен и настроен продукт «КриптоПро ЭЦП Browser plug-in», который применим в любом из современных браузеров с поддержкой сценариев JavaScript. Для взаимодействия с ним используется программное обеспечение, написанное на языке JavaScript. Кроме того, установлен и настроен криптопровайдер «КриптоПро CSP 3.6.6497», отвечающий за реализацию ЭП в соответствии с российскими криптографическими стандартами. Архитектура программной части представлена на рис. 2.

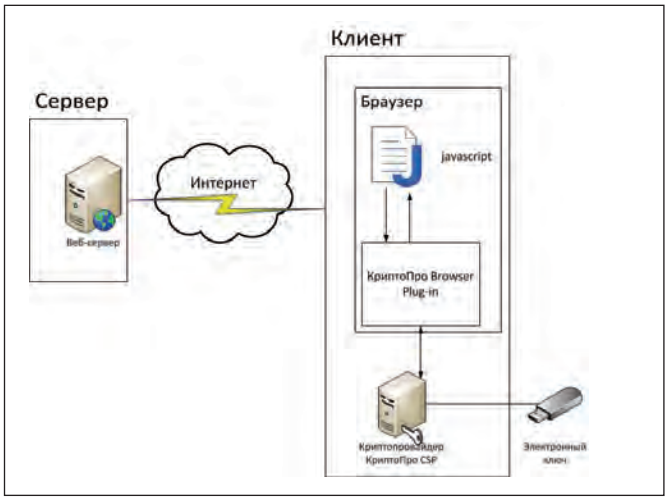

Рис. 2. Архитектура программной части

В «КриптоПро ЭЦП Browser plug-in» реализован набор объектов, предназначенный для создания и проверки сообщений, подписанных усовершенствованной подписью и удовлетворяющих стандарту ETSI TS 101 733 «Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)». На настоящий момент интерфейс поддерживает создание подписей типа CAdES BES и CAdES-X Long Type 1.

Для активации объектов КриптоПро Browser plug-in необходимо создать на странице скрытый элемент:

<object id=»cadesplugin» type=»application/x-cades» class=»hiddenObject»></object>.

При загрузке страницы проверяется наличие установленного плагина и выводится соответствующее сообщение. Проверка производится с помощью функции CheckForPlugIn(). После успешной активации плагина вызывается функция, отображающая список сертификатов для создания подписи.

Функция SignCreate() отвечает за создание подписи. В качестве параметров в функцию передаются сертификат и само сообщение, которое необходимо подписать. Для создания подписи вначале требуется создать объекты CPSigner и CadesSignedData, необходимые для генерации и проверки усовершенствованной электронной подписи, а также дополнить обычную подпись до усовершенствованной:

```
var oSigner = CreateObject(«CAdESCOM.CPSigner»);
var oSignedData = CreateObject(«CAdESCOM.CadesSignedData»);
```

Непосредственно за подпись отвечает функция SignCades():

```
Var sSignedMessage = oSignedData.SignCades(oSigner,
CADESCOM_CADES_X_LONG_TYPE_1);
```

которая в качестве параметров принимает:

- объект CPSigner, который будет использован для создания подписи;
- тип усовершенствованной подписи;
- вид подписи (по умолчанию совмещенная).

Результатом выполнения функции является сообщение, совмещенное с электронной подписью в виде Base64-строки.

Для доказательства момента подписи используются штампы времени, соответствующие международной рекомендации RFC 3161 — «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

Для добавления метки времени в подпись используется параметр TSAAddress из объекта CPSigner:

```
oSigner.TSAAddress = «http://cryptopro.ru/tsp/»;
```

Доказательства действительности сертификата в момент подписи обеспечиваются вложением в реквизиты документа цепочки сертификатов до доверенного УЦ и OCSP-ответов. На эти доказательства также ставится штамп времени, подтверждающий их целостность в момент проверки.

За проверку ЭП отвечает функция VerifyCades() из объекта CadesSignedData:

```
oSignedData.VerifyCades(sSignedMessage, CADESCOM_CADES_X_LONG_
TYPE_1);
```

принимающая в качестве параметров:

- сообщение вместе с совмещенной подписью;
- тип усовершенствованной подписи.

Кроме того, функция VerifyCades() позволяет проверить усовершенствованную подпись на соответствие заданному типу подписи.

При успешной проверке выводится информация о сообщении, статусе сертификата, данные о лице, подписавшем сообщение, и времени подписи.

СПИСОК ЛИТЕРАТУРЫ:

1. *Голдовский И. М.* Безопасность платежей в Интернете. СПб.: Питер, 2001. – 240 с.
2. Федеральный закон РФ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».