УДК 681.3

ОСОБЕННОСТИ РЕАЛИЗАЦИИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА НА БАЗЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА «КРИПТОПРО УЦ»

В.В. Резниченко

PECULIARITIES OF CERTIFICATION AUTHORITY IMPLEMENTATION ON THE BASIS OF HARDWARE AND SOFTWARE SYSTEM “CRYPTOPRO CA”

V.V. Reznichenko

Описан программно-аппаратный комплекс «КриптоПро УЦ» компании ООО «Крипто-Про», включающий в себя все необходимые компоненты для реализации удостоверяющего центра. Комплекс позволяет выдавать сертификаты электронной подписи в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94. Выделены основные функциональные компоненты, указаны особенности реализации удостоверяющего центра.

Ключевые слова: удостоверяющий центр, электронная подпись, программно-аппаратный комплекс.

Hardware and software system “CryptoPro CA” by LLC “Crypto-Pro”, consisting of the components, which are necessary for the implementation of certification authority, is described in the article. The system issues certificates of a digital signature in accordance to the All Union State Standards P 34.10-2001 and P 34.11-94. Basic functional components are pointed out; peculiarities of certification authority implementation are shown.

Keywords: certification authority, digital signature, hardware and software system.

Согласно Федеральному закону от 06.04.2011 г. № 63-ФЗ «Об электронной подписи», удостоверяющий центр – это «юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом» [1]. В рамках Закона удостоверяющему центру отводится роль доверенного арбитра при выдаче сертификатов ключа электронной подписи.

В общем случае сертификат электронной подписи может быть выдан программными средствами операционной системы MicrosoftWindows либо получен каким-то другим способом с помощью соответствующего математического алгоритма. В этом случае электронная подпись, согласно закону, называется неквалифицированной электронной подписью. «Неквалифицированность» в данном случае подразумевает под собой то, что эта электронная подпись будет иметь юридическое значение только среди участников электронного документооборота, которые заранее договорились и подтвердили подлинность данной электронной подписи. Другим видом электронной подписи является квалифицированная электронная подпись. Ее отличие от неквалифицированной состоит в том, что сертификат такой электронной подписи выдается аккредитованным удостоверяющим центром. Удостоверяющий центр проходит аккредитацию в соответствующих федеральных службах и получает статус доверенного удостоверяющего центра. Электронные документы, подписанные квалифицированной электронной подписью, признаются документами, равнозначными документам на бумажном носителе, подписанными собственноручно.

В условиях повсеместного развития электронного документооборота увеличилось количество аккредитованных удостоверяющих центров. Компания ООО «Крипто-Про» (http://www.cryptopro.ru) поставляет на рынок программно-аппаратный комплекс «КриптоПро УЦ», который включает в себя все необходимые компоненты для реализации удостоверяющего центра. Данный комплекс позволяет выдавать сертификаты электронной подписи в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94.

Концепция построения удостоверяющего центра на базе программно-аппаратного комплекса «КриптоПро УЦ» заключается в разделении удостоверяющего центра на три функциональных компонента. Первый функциональный компонент – центр сертификации (ЦС). Этот компонент предназначен собственно для выдачи сертифика-

Резниченко Вадим Валерьевич – доцент кафедры безопасности информационных систем, Южно-Уральский государственный университет; kin@ kb.susu.ac.ru

Reznichenko Vadim Valerievich – associate professor of the Department of Information Systems Security, South Ural State University; kin@kb.susu.ac.ru

тов цифровой подписи. Второй компонент – центр регистрации (ЦР). Этот компонент служит своеобразным связующим звеном между администратором удостоверяющего центра и центром сертификации. Третий компонент – автоматизированное рабочее место (АРМ) администратора. Этот компонент предназначен для управления всем удостоверяющим центром. Есть еще четвертый компонент, который не входит в основную структуру удостоверяющего центра. Этот компонент – АРМ разбора конфликтных ситуаций. Он предназначен для решения спорных ситуаций, возникающих во время электронного документооборота.

Особенностью реализации удостоверяющего центра на базе программно-аппаратного комплекса «КриптоПро УЦ» является то, что компоненты ЦС, ЦР и АРМ администратора должны быть обязательно установлены на физически отдельные ПЭВМ. Это связано с тем, что требуется обеспечить недоступность ЦС извне. ПЭВМ соединяются в локальную вычислительную сеть, при этом соединения настраиваются таким образом, чтобы ЦС был недоступен для входа на него по сети. АРМ администратора соединяется с ЦР, ЦР соединяется с ЦС. Таким образом, администратор удостоверяющего центра, работая на АРМе администратора, управляет удостоверяющим центром, но не имеет доступа напрямую к ЦС. Требование к недоступности ЦС вытекает из того, что ЦС содержит корневой сертификат (то есть сертификат, на базе которого формируются все остальные сертификаты), базу выданных сертификатов, а также список отозванных сертификатов.

Для реализации такой схемы взаимодействия применяется защищенный шифрованный сетевой протокол TLS [2]. Для развертывания удостоверяющего центра устанавливают три отдельных ПЭВМ и соединяют их в локальную вычислительную сеть. Далее на эти ПЭВМ устанавливают компоненты удостоверяющего центра: центр сертификации, центр регистрации и АРМ администратора. Компоненты представляют собой специализированное программное обеспечение. Затем при помощи протокола TLS устанавливают соединение между ЦС и ЦР, затем между АРМ администратора и ЦР.

По данной схеме удостоверяющий центр функционирует следующим образом: для выдачи пользователю нового квалифицированного сертификата цифровой подписи администратор при помощи АРМ администратора создает нового пользователя. Далее он формирует запрос на ЦС для выдачи сертификата. Запрос поступает в ЦР, затем ЦР передает его в ЦС. Центр сертификации обрабатывает запрос и возвращает созданный сертификат в ЦР. ЦР передает сертификат в АРМ администратора, где он может быть сохранен на защищенный носитель, а также распечатана копия открытой части ключа подписи.

Для создания цифровой подписи используется отдельное программное обеспечение, поставляемое все той же компанией ООО «Крипто-Про», – средство криптографической защиты информации «Крипто-ПроCSP». Особенностью данного программного обеспечения является использование шифровального алгоритма в соответствии с ГОСТ 28147-89.

АРМ разбора конфликтных ситуаций является совершенно автономным компонентом и может быть установлен на другую отдельную ПЭВМ или на АРМ администратора.

Можно отметить ряд достоинств программно-аппаратного комплекса «КриптоПро УЦ». Данный комплекс является готовым решением «из коробки» и не требует дополнительных затрат на доработку. Продуманная схема функционирования позволяет администратору со своего рабочего места эффективно управлять удостоверяющим центром (выдавать, удалять, приостанавливать действие сертификатов цифровой подписи, вести реестр сертификатов, выпускать список отозванных сертификатов), при этом компоненты ЦР и ЦС могут быть расположены удаленно в других помещениях, других зданиях и т. п. Также данная схема позволяет использовать несколько ЦР в случае, если для регистрации новых пользователей будет развернуто несколько удаленно расположенных точек приема заявок на получение сертификатов цифровой подписи, при этом используется один ЦС. Возможно построение удостоверяющего центра как с подключением к Интернету, так и без него. В случае подключения к Интернету возможно использование web-сервиса, позволяющего пользователям самостоятельно удаленно получать сертификаты цифровой подписи [3].

У данной реализации схемы взаимодействия имеется ряд недостатков. Во-первых, необходимость развертывания как минимум трех ПЭВМ. Во-вторых, ввиду использования для взаимодействия протокола TLS возникают сложности с установкой соединения между компонентами удостоверяющего центра. Вообще, ввиду достаточно сложной структуры, установка и настройка комплекса «КриптоПро УЦ» представляет собой нетривиальную задачу. Могут возникать конфликты на уровне операционной системы, сетевых протоколов, а также самих компонентов удостоверяющего центра.

Программно-аппаратный комплекс «КриптоПро УЦ» позволяет развернуть удостоверяющий центр, удовлетворяющий современным техническим и юридическим требованиям в соответствии с законодательством Российской Федерации. Развертывание, установка и наладка комплекса сопряжена с определенными техническими сложностями.

Литература

1. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи». – Доступ из справ.-правовой системы «КонсультантПлюс».

2. Технические средства и методы защиты информации: учеб. для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство „Машиностроение“», 2009. – 508 с.

3. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. – М.: Изд-во стандартов, 2000. – 22 с.

Поступила в редакцию 1 июня 2012 г.