УДК 681.3.06

МОДЕЛИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

© 2017 В. Д. Камакин

Воронежский институт высоких технологий (г. Воронеж, Россия)

В статье представлены результаты проведенного анализа моделей цифровой подписи.

Ключевые слова: электронная цифровая подпись, модель ЭЦП.

Сертификат открытого ключа ЭП (сертификат ключа подписи) – документ, выданный и заверенный удостоверяющим центром, подтверждающий принадлежность открытого ключа ЭП определенному лицу. Открытый ключ (рис. 1) указывается в сертификате и доступен каждому.

Сертификат выдается на имя владельца, который может быть как физическим, так и юридическим лицом, владеющим закрытым ключом ЭП, соответствующим открытому ключу. Сертификат – это небольшой файл, состоящий из следующих частей:

- даты начала и окончания срока его действия;
- фамилия, имя и отчество (если имеется) – для физических лиц, наименование и место нахождения – для юридических лиц;
- ключ проверки электронной подписи;
- наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи;
- иная информация – для квалифицированного сертификата.

Удостоверяющий центр хранит справочник регистрационных записей открытых ключей, к которому вправе обратиться любой участник информационного обмена. Каждый сертификат заверяется подписью центра. Схема проверки подлинности сертификата показана на рисунке 2.

Центры по удостоверению подлинности ЭП – юридические лица, обладающие соответствующими правомочиями на удостоверение принадлежности экземпляра открытого ключа ЭП конкретному владельцу сертификата.

Нельзя забывать, что, несмотря на все преимущества, у ЭП, как, впрочем, и у любого другого средства криптографической защиты, есть одна достаточно неприятная особенность: используемую ключевую пару необходимо периодически менять, пока ее не успели скомпрометировать злоумышленники. То есть, условно говоря, через год (два, три), после того как абонент удостоверяющего центра передаст ему на сертификацию свой открытый ключ, все старые документы могут автоматически оказаться «вне закона» – ведь теперь будет работать новая пара ключей.

В случае, если после истечения срока действия старых ключей возникнет какой-нибудь юридический спор и для его разрешения потребуется один из документов, подписанных с использованием старого ключа, закон «Об электронной подписи» предлагает принцип перехода к режиму архивного хранения ключей в удостоверяющем центре в соответствии с российским законодательством об архивах и архивном деле.

Для обеспечения возможности использования криптографии с открытым ключом, необходимо гарантировать, что каждый закрытый и открытый ключ управляется корректным образом. Существует две модели организации инфраструктуры сертификатов: централизованная (инфраструктура открытых ключей, англ. PKI – Public Key Infrastructure) и децентрализованная (реализуемая на основе так называемых сетей доверия, получившая наибольшее распространение в сетях PGP).

Камакин Виктор Дмитриевич – ВИВТ-АНОО ВО, kam13akin2045@yandex.ru.

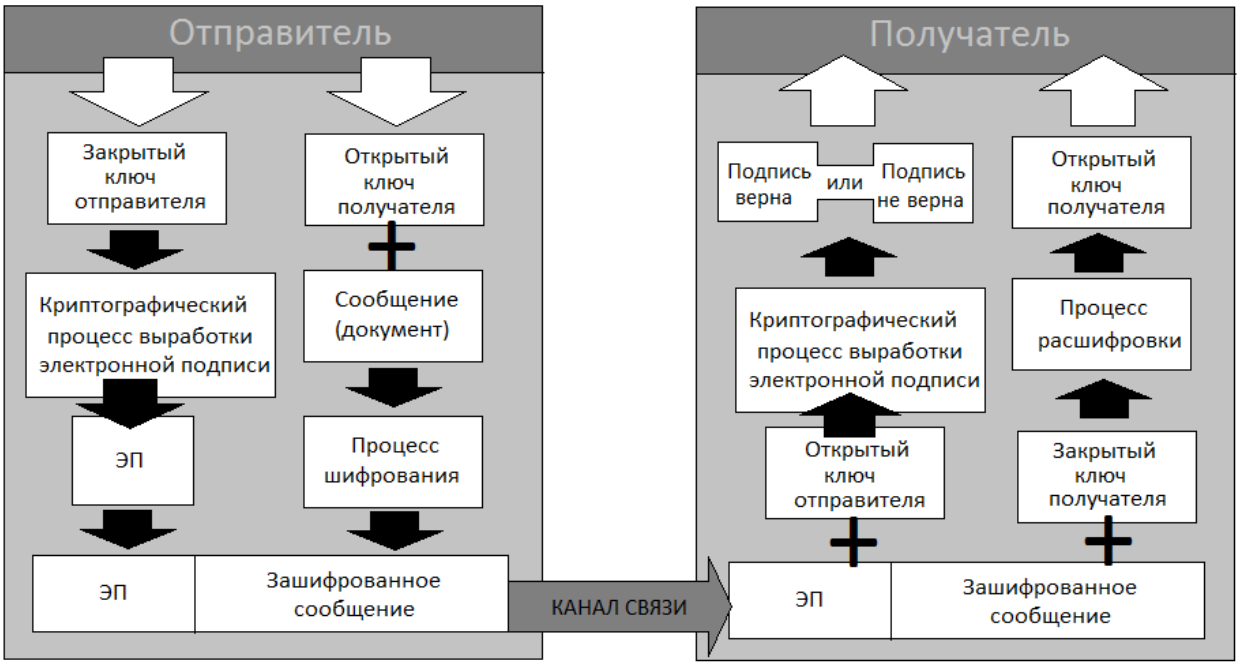

Рисунок 1. Постановка и проверка ЭП под электронным документом с одновременной ассиметричной шифрацией и расшифровкой документа.

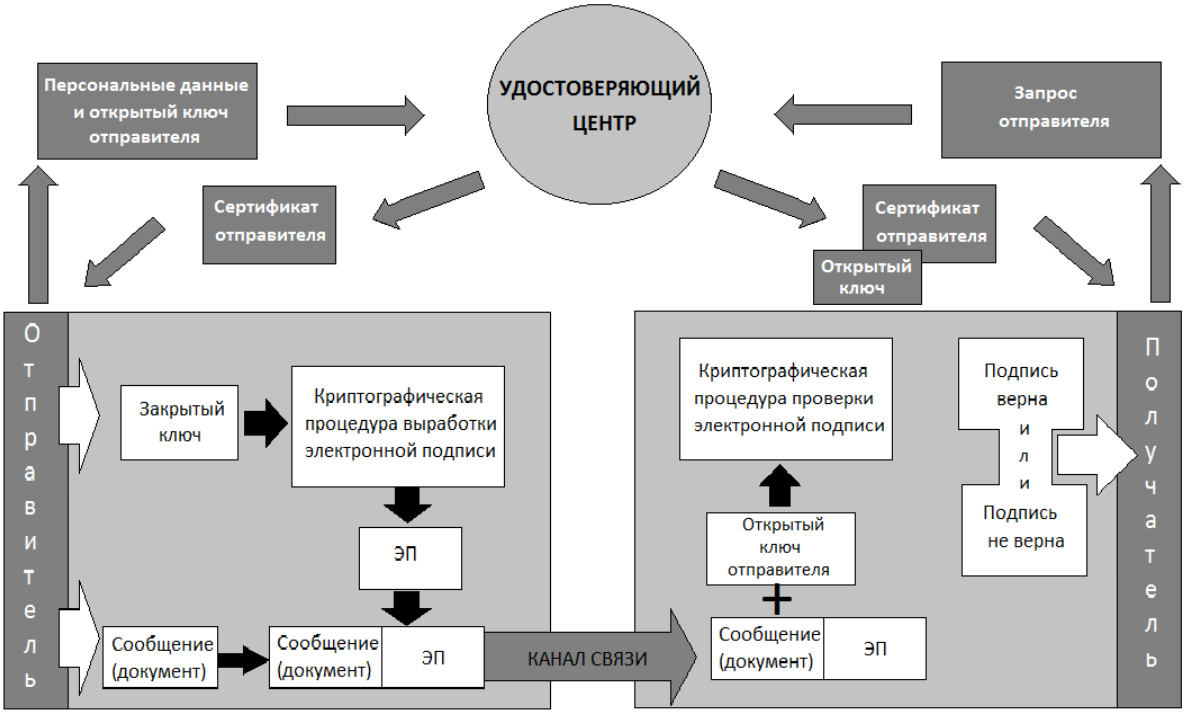

Рисунок 2. Постановка и проверка ЭП при участии удостоверяющего центра.

Описанная централизованная модель организации инфраструктуры сертификатов ориентирована на использование так называемой инфраструктуры открытых ключей (англ. PKI – Public Key Infrastructure). Кроме владельцев и пользователей цифровых сертификатов, эффективный PKI должен включать целый ряд других элементов. Это центры сертификации и регистрации, архив сертификатов, а также системы:

– аннулирования сертификатов;

– создания резервных копий и восстановления ключей;

– автоматической корректировки пар ключей и сертификатов;

– управления историей ключей;

– поддержки взаимной сертификации разных центров;

– поддержки механизма невозможности отказа от электронных подписей;

– преобразования форматов (необходима при обмене документами многих участников, использующих разное программное обеспечение) и т. д.

Подобная инфраструктура давно прошла испытание временем за рубежом и уже более 10 лет достаточно активно используется в России организациями, ведущими защищенный электронный документооборот.

Чтобы проблема совместимости криптографических приложений на уровне PKI не возникала, все ее участники должны придерживаться единой структуры и форматов представления данных в составе цифрового сертификата. Этой цели служит международный стандарт X.509, разработанный Международным комитетом по телекоммуникациям (ITU-T) и авторитетной общественной международной организацией Internet Engineering Task Force (IETF). Опубликованные этими уважаемыми организациями рекомендации, определяющие форматы цифровых сертификатов, широко и успешно используются не только зарубежными, но и многими российскими криптосистемами.

Другая модель организации инфраструктуры сертификатов – децентрализованная, реализуемая на основе так называемых сетей доверия, получила наибольшее распространение в сетях PGP.

Принятие нового закона в 2011 г. было обусловлено приведением российского законодательства в соответствие с международными стандартами. Так, Федеральный закон «Об электронной подписи» значительно расширил сферу применения электронной подписи, разрешил ее получение юридическим лицам, закрепил систему аккредитации удостоверяющих центров. Одним из главных новшеств стало введение нескольких видов электронной подписи – простой и усиленной, тогда как Простая электронная подпись – это подпись, которая посредством использования кодов, паролей и иных средств подтверждения подтверждает факт формирования электронной подписи определенным лицом. Она является самой доступной из всех видов электронной подписи и формируется посредством схемы "логин-пароль" или использования одноразового пароля.

Простая электронная подпись позволяет установить только личность лица, подписавшего документ, но не факт изменения содержимого документа после его подписания, что значительно ограничивает сферу ее использования.

Помимо простой электронной подписи существует также усиленная, которая может быть квалифицированной и неквалифицированной.

Неквалифицированной усиленной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи (ч. 3 ст. 5 Федерального закона «Об электронной подписи»).

Для использования усиленной электронной подписи ее владелец получает два ключа. Ключ электронной подписи (закрытый ключ) служит для создания электронной подписи документа и, как правило, хранится на обособленном носителе. Одним из распространенных носителей ключа электронной подписи является токен (USB-ключи E-token, Rutoken). Он представляет собой компактное мобильное USB-устройство, на котором хранится подпись. Токен имеет защищенную область памяти, и получить доступ к ней для использования электронной подписи может только владелец электронной подписи, знающий код доступа к токену. Этим обеспечивается подтверждение того, что документ подписан конкретным лицом. Обычно при подписании электронного документа он направляется на токен, внутри которого генерируется подпись и прочно связывается с содержимым документа, а потом подписанный документ выдается обратно владельцу ключа. Закрытый ключ, таким образом, не покидает свой носитель, что обеспечивает безопасность при применении электронной подписи. Кроме того,

связывание содержимого документа с электронной подписью позволяет определить, не вносились ли изменения в документ после его подписания.

Закрытый ключ связан с ключом проверки электронной подписи (открытый ключ). Именно этот ключ использует адресат электронного документа, чтобы с его помощью удостовериться в действительности подписи и отсутствии изменений документа после его подписания. В удостоверяющем центре, выдавшем сертификат ключа проверки электронной подписи, находится дубликат открытого ключа на случай споров о подлинности подписи.

Квалифицированная усиленная электронная подпись отличается от неквалифицированной тем, что ее сертификат ключа проверки подписи (квалифицированный сертификат) создан и выдан удостоверяющим центром, аккредитованным при Минкомсвязи России. Программное средство криптозащиты такой электронной подписи, а также аппаратное средство криптозащиты (токен) сертифицированы ФСБ России. Она считается самым защищенным видом электронной подписи и требуется для электронного взаимодействия с государственными органами в подавляющем большинстве случаев.

Если аккредитованный удостоверяющий центр допустит причинение убытков третьим лицам, доверившимся указанной в сертификате ключа информации, или информации, содержащейся в реестре сертификатов этого удостоверяющего центра, его ответственность обеспечивается суммой не менее 1,5 млн руб.

ЭП используется для следующих целей:

– Доказательное подтверждение авторства документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесенные изменения», «метка времени» и т. д.

– Контроль целостности передаваемого документа. При любом случайном или преднамеренном изменении документа изменится подпись, следовательно, она станет недействительной.

– Защиту от изменений (подделки) документа.

– Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.

Все эти свойства электронной подписи позволяют использовать ее для решения следующих задач:

– организация юридически значимого электронного документооборота;

– представление обязательной отчетности перед государственными учреждениями, контролирующими органа-ми;

– декларирование товаров и услуг (таможенные декларации, розничная продажа алкогольной продукции;

– регистрация сделок по объектам недвижимости;

– использование в банковских системах;

– в расчетных и трейдинговых системах;

– электронная торговля и госзаказы;

– в системах обращения к органам власти;

– контроль исполнения государственного бюджета;

– при организации выборов.

Говорить о целесообразности использования ЭП в общих словах – несколько не правильно, так как определённые направления имеют и недостатки, и положительные моменты.

ЭП для сдачи отчетности практически не имеет преимуществ, если расценивать их с глобальной точки зрения. Тем не менее, сдача отчетности, подпись электронной документации при помощи этого инструмента экономит время, сохраняя юридическую значимость, так же, как и бумажный документ.

Недостатками ЭП по сравнению с подписью обычного документа, что называется «от руки», является высокая цена программного обеспечения, не разрешенная проблема среднесрочного и длительного хранения электронной документации, заключение и исполнение трансграничной отчетности, справок, сертификатов качества, свидетельств и т. д.

Другое дело с использованием электронной подписи для идентификации личности на торговых площадках, проведения тендеров, торгов и аукционов внутри страны. Ряд европейских государств, в особенности Германия, Швеция, Бельгия и

Дания, отмечают положительный стремительный рост динамики использования ЭП.

Прогноз на будущее также вполне позитивен, но мировому сообществу, странам ЕС, России, странам Азии придется решить немало вопросов о стандартизации ЭП и создании единого экономического пространства для эффективного, и не менее важного – оправданного, использования ЭП та территории стран содружества.

Сегодня электронная подпись практически на 100 % заменила идентификацию сторон при заключении договоров, а, следовательно, стала заменой обычной ручной подписи.

ЛИТЕРАТУРА

1. Кострова В. Н. Оптимизация распределения ресурсов в рамках комплекса общеобразовательных учреждений / В. Н. Кострова, Я. Е. Львович, О. Н. Мосолов // Вестник Воронежского государственного технического университета. – 2007. – Т. 3. – № 8. – С. 174-176.

2. Преображенский Ю. П. Разработка методов формализации задач на основе семантической модели предметной области / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 075-077.

3. Львович И. Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А. Воронов, Ю. П. Преображенский // Информация и безопасность. – 2006. – Т. 9. – № 1. – С. 36-39.

4. Черников С. Ю. Использование системного анализа при управлении организациями / С. Ю. Черников, Р. В. Корольков // Моделирование, оптимизация и информационные технологии. – 2014. – № 2 (5). – С. 16.

5. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

6. Фомина Ю. А. Принципы индексации информации в поисковых системах / Ю. А. Фомина, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 98-100.

7. Преображенский Ю. П. Информационная безопасность – вызовы современного мира / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2017. – № 2 (21). – С. 60-63.

8. Маричев А. В. Вопросы социальной инженерии в корпоративной информационной безопасности / А. В. Маричев, И. В. Любимов, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2017. – № 2 (21). – С. 64-67.

9. Львович И. Я. Основы информатики / И. Я. Львович, Ю. П. Преображенский, В. В. Ермолова // Воронеж, Издательство: Воронежский институт высоких технологий (Воронеж), 2014. – 339 с.

10. Паневин Р. Ю. Структурные и функциональные требования к программному комплексу представления знаний / Р. Ю. Паневин, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 061-064.

THE COMPARATIVE ANALYSIS OF CLASSICAL AND SPECIAL ALGORITHMS AND SCHEMES OF THE DIGITAL SIGNATURE

© 2017 V. D. Kamakin

Voronezh Institute of High Technologies (Voronezh, Russia)

The analysis of classic and special digital signature algorithms is carried out.

Keywords: electronic digital signature algorithms.