УДК 004.089

А.Г. Сабанов

Аутентификация при электронном обмене конфиденциальными документами

Рассмотрена задача аутентификации пользователей при электронном взаимодействии в двух типах информационных систем. Предложены требования к идентификации и аутентификации для различных групп участников электронного взаимодействия в информационных системах общего пользования. Разработаны требования к способам аутентификации при применении различных видов электронной подписи.

Ключевые слова: аутентификация, идентификация, электронная подпись.

До недавнего времени задачи аутентификации в основном решались для корпоративных информационных систем (ИС), участниками электронного взаимодействия в которых является определенный круг лиц. В последние годы интенсивно развивается новый тип ИС – информационные системы общего пользования (ИСОП), «участниками электронного взаимодействия в которых является неопределенный круг лиц и в использовании которых этим лицам не может быть отказано» (ст. 2 п. 13 Федерального закона [1]). Размеры ИСОП и число их участников могут достигать гигантских размеров. Одним из примеров таких систем является Интернет. В отличие от Интернета, где изначально был реализован принцип анонимности пользователя, в большинстве ИСОП (системы электронной коммерции, государственных услуг для граждан и организаций и т.д.) за исключением случаев информирования (получения открытой информации) необходимо обеспечение надежных механизмов управления доступом пользователей системы. Как показано в работе [2], решение данной задачи невозможно без применения средств автоматической идентификации – процедуры распознавания субъекта по его уникальному идентификатору, присвоенному данному субъекту ранее и занесенному в базу данных в момент регистрации субъекта в качестве легального пользователя системы. В случаях, когда в системе обрабатывается и хранится конфиденциальная информация (служебная тайна, персональные данные и т.п.), доступ пользователей должен быть минимально достаточен и строго персонифицирован, следовательно, необходимо использовать надежные средства аутентификации – комплекса процедур проверки подлинности входящего в систему объекта, предъявившего свой идентификатор.

Обычно проверка состоит в процедуре обмена между входящим в систему объектом и ресурсом, отвечающим за принятие решения («да» или «нет»). Данная проверка, как правило, производится с применением криптографических преобразований, которые нужны, с одной стороны, для того, чтобы достоверно убедиться в том, что субъект является тем, за кого себя выдает, с другой стороны – для защиты трафика обмена субъект–система от злоумышленника. Таким образом, идентификация и аутентификация как сервисы безопасности являются взаимосвязанными процессами распознавания и проверки подлинности пользователей. Именно от корректности решения этих двух задач (распознавания и проверки подлинности) зависит, можно ли разрешить доступ к ресурсам системы конкретному пользователю, т.е. будет ли он авторизован. Корректность решения задачи аутентификации особенно критична при применении электронной подписи – тот ли субъект ставит подпись под документом? В отличие от США [3] и Организации экономического сотрудничества и развития (сокр. ОЭСР, в английском варианте *Organization for Economic Co-operation and Development, OECD*) [4] в нормативных документах Российской Федерации пока нет требований к технологиям и способам аутентификации при электронном взаимодействии.

В данной работе делается попытка сформулировать такие требования с учетом мирового опыта и действующего в России законодательства.

Особенности решения задач идентификации и аутентификации в ИССОП. Задачи идентификации и аутентификации для локальных сетей и корпоративных систем к настоящему времени хорошо изучены и имеют ряд решений, проверенных на практике. Например, общетеоретические и практические задачи для локальных систем достаточно подробно рассмотрены в работах [5] и [6]. В работе [7] методы идентификации и аутентификации классифицированы с точки зрения применяе-

мых технологий. В работе [6] рассмотрены вопросы решения задач интеграции систем аутентификации для распределенных корпоративных систем. В отличие от корпоративных систем, в которых участники информационного взаимодействия становятся легальными пользователями системы после заключения трудового договора, обязывающего их выполнять определенные правила работы с вычислительной техникой и информацией, пользователи ИСОП, как правило, не связаны столь строгими договорными отношениями и вытекающими из них регламентами. С другой стороны, в ИСОП для внешних пользователей системы, как правило, невозможно осуществлять хорошо развитые к настоящему времени корпоративные политики безопасности, включающие в себя кроме нормативной базы и организационных мер необходимые настройки корпоративного системного, прикладного и специального программного обеспечения. Например, если в информационной системе обрабатываются персональные данные, то доступ пользователей должен быть обязательно разделен. При этом для идентификации пользователей согласно «лучшим практикам» используется цифровой сертификат – «электронный паспорт», применяется механизм строгой двухфакторной аутентификации (один фактор – персональная смарт-карта, второй фактор – знание PIN-кода) легальных пользователей, основанный на применении технологии электронной подписи [8]. Для этого на рабочей станции пользователя, как минимум, должны быть установлены и настроены следующие компоненты: легально приобретенная операционная система, поддерживающая PKI (Public Key Infrastructure) для работы с открытыми ключами сервера и пользователей, драйвера для работы со смарт-картой и считывателем, CSP (Crypto Service Provider) для выполнения на рабочей станции криптографических преобразований и установления защищенного канала (при необходимости). У пользователя в данном случае, как минимум, должна быть персонифицированная готовая к работе смарт-карта, на которой должны храниться необходимые закрытые ключи и сертификаты (в общем случае два сертификата – доступа и электронной подписи).

Для пользователя ИСОП, не связанного договорными отношениями с владельцем ИСОП, такой набор компонент и обязательность при этом проверки на чистоту от вирусов и троянов компьютера нужны далеко не всегда (например, упомянутый выше случай информирования), а главное, такую конфигурацию в домашних условиях редко кто сможет обеспечить.

Согласно ст. 2 Федерального закона №63-ФЗ «Об электронной подписи» [1] участниками информационного взаимодействия могут быть государственные органы, органы местного самоуправления, организации и граждане. Попробуем сформулировать требования к идентификации и аутентификации для этих групп участников взаимодействия.

Требования к идентификации и аутентификации. Рассмотрим виды электронной подписи, введенные Федеральным законом №63-ФЗ. Согласно ст. 5 указанного закона видами электронных подписей являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее – неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее – квалифицированная электронная подпись).

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

Неквалифицированной 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.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Перейдем к вопросам применения этих формулировок для практических запросов на государственные услуги. Если запрос на услуги не персонифицирован (например, в простейшем случае не требует ответа ответственного лица), то идентификация не нужна. Соответственно, не требуется и аутентификация того, кто делает запрос.

Если запрос на государственную услугу персонифицирован, то требуется идентификация пославшего запрос. Если ответ подразумевает подпись ответственного лица, то вдобавок к обязательной идентификации требуется аутентичность запроса и ответа. Если подпись усиленная (с использованием неквалифицированного или квалифицированного сертификата), то соответственно требуется строгая аутентификация.

Для наглядности эти требования представлены в табл. 1.

Таблица 1

Требования к идентификации и аутентификации для участников информационного взаимодействия

Участники информационного взаимодействия	Идентификация	Аутентификация
Государственные органы	Да	Строгая
Органы местного самоуправления	Да	Строгая
Организации	Да	Да/Нет в зависимости от запроса
Граждане	Да/Нет в зависимости от запроса	Да/Нет в зависимости от запроса

Соответственно на основе анализа текста закона [1] и приведенных рассуждений мы можем сформулировать и требования к способам аутентификации. В случаях, когда ответ ответственного лица на запрос государственной услуги имеет правовые последствия (типичным примером является услуга подтверждения или перехода прав собственности на недвижимость), необходимо применять усиленную электронную подпись и квалифицированный сертификат. При этом требуется применение строгой двухфакторной аутентификации. Результаты для наглядности представлены в виде табл. 2.

Таблица 2

Требования к аутентификации в зависимости от вида электронной подписи

Виды подписи	Аутентификация
Простая	Да
Усиленная (неквалифицированный сертификат)	Строгая
Усиленная (квалифицированный сертификат)	Строгая

Действительно, в приведенной выше формулировке ст. 5 №63-ФЗ простая электронная подпись подразумевает аутентификацию источника, но не подразумевает проведения контроля целостности сообщения. Соответственно, если во время электронного взаимодействия применяется несколько подписей (например, простая электронная подпись и квалифицированная электронная подпись), то согласно принципу Кирхгофа (степень защищенности системы определяется степенью защищенности ее слабого звена) корректно решается только задача аутентификации источников, но не контроль целостности подписанных сообщений.

Заключение. В зависимости от назначения системы, степени конфиденциальности циркулирующей в ней информации и роли пользователей задачи автоматической идентификации и аутентификации претендентов на право авторизации в качестве пользователя ИСОП всегда требуют внимательного изучения. С одной стороны, это обусловлено тем, что в нормативных актах отсутствуют не только требования, но и рекомендации по выбору технологических решений для решения данной задачи. С другой стороны, существующее многообразие технологий, продвигаемых производителями с той или иной степенью успешности, может породить ошибки проектировщиков ИСОП с точки зрения обеспечения надежности функционирования и реальной защиты выбранных решений.

Ожидается, что предложенные требования к идентификации и аутентификации позволят существенно снизить риски мошенничеств при строительстве и эксплуатации ИСОП. В качестве разви-

тия данной работы и на ее основе можно будет сформулировать требования к доверенным сервисам создаваемого единого пространства доверия, необходимого для обеспечения юридической значимости документов при электронном взаимодействии.

Литература

1. Федеральный закон «Об электронной подписи» № 63-ФЗ от 7 апреля 2011 г. [Электронный ресурс]. – Режим доступа: http://www.customs-code.ru/tamoformlen/117-declelectron/6398-fz63, свободный (дата обращения: 24.10.2011).

2. Сарбуков А.Е. Аутентификация в компьютерных системах / А.Е. Сарбуков, А.А. Грушо // Системы безопасности. – 2003. – № 5(53). – С. 17–21.

3. Electronic Authentication Guideline. NIST Special Publication 800-63. April 2006. – 54 p. [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf, свободный (дата обращения: 24.10.2011).

4. OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication. OECD 2007. – 36 p. [Электронный ресурс]. – Режим доступа: http://www.oecd.org/dataoecd/32/45/38921342.pdf, свободный (дата обращения: 24.10.2011).

5. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений/ А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 616 с.

6. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учеб. пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия–Телеком, 2009. – 552 с.

7. Сабанов А.Г. Об интеграции средств аутентификации // Connect! Мир связи. – 2010 – №9. – С. 101–103. – (Первая часть); №10. – С. 113–115. – (Вторая часть).

8. Сабанов А.Г. Обзор технологий идентификации и аутентификации // Документальная электросвязь. – 2006. – № 17. – С. 23–27.

Сабанов Алексей Геннадьевич
Канд. техн. наук, зам. ген. директора ЗАО «Аладдин Р.Д.», г. Москва
Тел.: 8-985-924-52-09
Эл. почта: asabanov@mail.ru

Sabanov A.G.

About requirements to electronic interaction authentication

In this article there is an observation of new ways of users' authentication in the case of access to two types of information systems. There is suggested a requirements of wide-spread identification and authentication factors for different groups of electronic interaction users. Requirements to methods of authentication for different kinds of electronic signatures are designed.

Keywords: authentication, identification, electronic signature.
