Электронная цифровая подпись: что нужно знать

СЕРГЕЙ СИЛИН

В последнее время электронно-цифровая подпись (ЭЦП) получает все большее распространение в отечественных корпоративных информационных системах. Однако однобокое, как правило, техническое освещение вопросов применения ЭЦП не позволяет увидеть картину в целом, в силу чего возникла необходимость рассмотреть эту область “с высоты птичьего полета”. Не вдаваясь в детали, интересные только специалистам, мы постараемся рассказать о том, что позволяет и чего не позволяет реализовать электронно-цифровая подпись, а также дать практические рекомендации по применению ЭЦП в системах электронного документооборота, потребность в которых сегодня ощущается все сильнее.

По общему мнению, собственноручная подпись на бумажном документе решает следующие задачи:

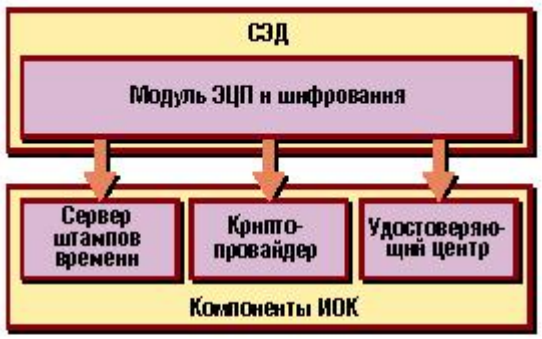
убедить читателя в том, что человек, подписавший документ, сделал это сознательно (*подпись достоверна*);

доказать, что именно этот человек, и никто другой, сознательно подписал документ (*подпись неподдельна*);

будучи частью документа, защитить ее от мошеннического переноса в другой документ (*подпись невозможно использовать повторно*);

защитить и сам документ (*подписанный документ невозможно изменить*);

обеспечить материальность подписи и документа, гарантирующую, что человек, подписавший документ, не сможет утверждать впоследствии, что документ подписан не им (*от подписи нельзя отказаться*).



Функционирование СЭД с ЭЦП обеспечивают четыре компонента: программно-аппаратный комплекс СЭД, имеющий в составе модуль “ЭЦП и шифрование”, программно-аппаратные комплексы службы штампов времени и удостоверяющего центра, а также несколько криптопровайдеров

Однако, как показывает практика, собственноручная подпись на бумажном документе по самой своей природе оставляет лазейки для мошенников. Недаром для затруднения их действий на бланки документов наносят специальные защитные знаки, применяют нумерацию и скрепление листов, а кроме того, наряду с самой подписью используют собственноручное написание фамилии, имени, отчества на документе и т. п. Одним словом, при всех ее достоинствах собственноручная подпись обладает и целым рядом недостатков.

Как результат проникновения компьютерных технологий во все сферы человеческой деятельности возникла потребность реализовать аналог собственноручной подписи человека в электронном виде. Эта задача была успешно решена. В основе решения лежат разработанные в середине 1970-х гг. криптографические алгоритмы с открытым ключом, которые базируются на сложном математическом аппарате.

При этом ЭЦП устранила большинство проблем, свойственных подписи на бумажном документе, и обеспечила электронному документу следующие важнейшие характеристики:

подлинность — подтверждение авторства документа;

целостность — документ не может быть изменен после подписания;

неотрицание авторства (неотрекаемость) — автор впоследствии не сможет отказаться от своей подписи.

Наиболее широкое применение сегодня ЭЦП находит в документационном обеспечении управления (ДОУ), в платежных системах, электронной торговле и бухгалтерии. Из перечисленных направлений наиболее востребованной и сложной является задача автоматизации ДОУ организаций — главная цель создания систем электронного документооборота (СЭД). Именно на нем мы и сосредоточим свое внимание в статье. Однако прежде необходимо уточнить, что понимается под использованием ЭЦП, имея в виду две основные его схемы:

подписание электронного сообщения при его передаче и проверка подписи отправителя после получения, то есть **защищенная передача документа**. Часто подобную схему воспринимают как юридически значимый документооборот, что является глубоким заблуждением. Защита электронного сообщения посредством ЭЦП — вещь, безусловно, полезная и нужная, но для обеспечения полноценного документооборота совершенно недостаточная;

использование ЭЦП **во всем жизненном цикле** электронного документа — при его создании, согласовании, утверждении, ознакомлении с ним и т. д. Только в том случае, когда автоматизируется полный жизненный цикл документа и ЭЦП является его неотъемлемой частью, можно говорить об использовании полноценной, т. е. юридически значимой **системы электронного документооборота**.

Далее будем рассматривать юридически значимые СЭД.

СЭД с поддержкой ЭЦП: в чем выгоды

Основная отличительная черта СЭД с поддержкой ЭЦП от СЭД без таковой поддержки состоит в том, что электронные документы, снабженные ЭЦП, являются доказательствами: они документируют решение или какой-либо факт. Если при возникновении конфликтной ситуации существует электронный документ, подписанный ЭЦП, то на его основе можно провести расследование внутри организации, а при необходимости — и с привлечением третьей

стороны (например, в арбитражном суде). СЭД, не предусматривающие ЭЦП, такой возможности не предоставляют.

Электронный документ — это документ, подготовленный с использованием системы электронного документооборота, зафиксированный на материальном носителе в виде объекта СЭД и снабженный реквизитами, с помощью которых можно идентифицировать место, время создания и автора документа.

: Пользователи СЭД без ЭЦП вынуждены доверять системе, системным администраторам, другим участникам работы с документами, причем без каких-либо веских на то оснований. При наличии же ЭЦП основания для доверия есть — это криптографические алгоритмы и протоколы.

Доказательность электронных документов имеет два важных следствия:

возникает возможность полностью отказаться от бумажных документов при условии, что это не противоречит действующему законодательству (некоторые типы документов требуется иметь в бумажном виде). Это позволяет избежать дублирования информации на различных носителях, обеспечивает надежное хранение данных и предотвращает утечку конфиденциальной информации;

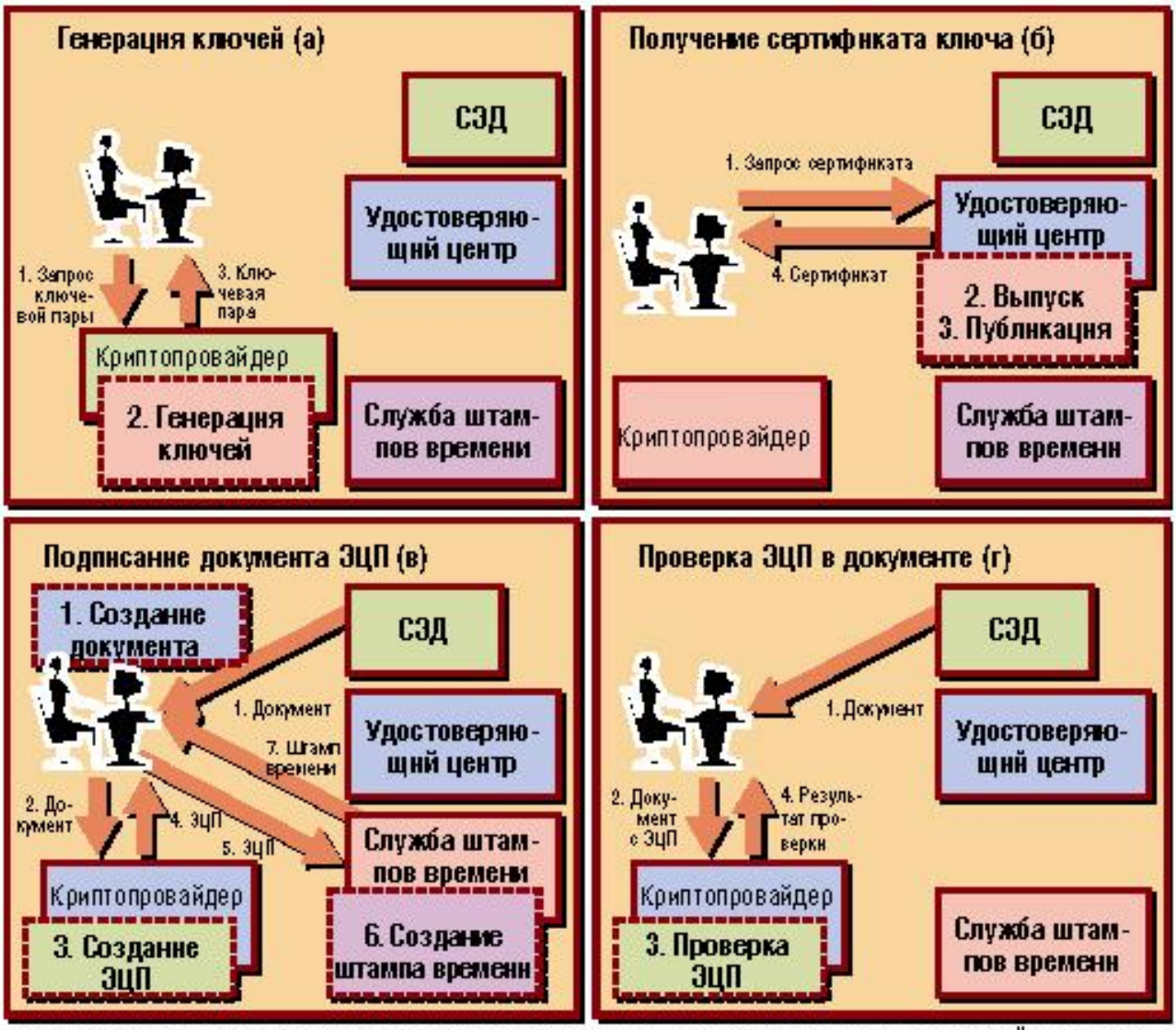
отпадает надобность в физической передаче сотрудникам бумажных документов, что многократно ускоряет процессы принятия решений по документам и доведения решений руководства до сотрудников.

Принятие федерального закона “Об электронно-цифровой подписи” стало точкой отсчета для введения в оборот термина “юридически значимый электронный документооборот”. Сейчас этот термин трактуется весьма широко, что часто вызывает недоразумения во взаимоотношениях заказчиков и разработчиков СЭД. Чтобы лучше понять этот термин, необходимо развеять некоторые заблуждения, касающиеся применения ЭЦП в СЭД и обеспечения юридической значимости документа: по сути электронный документ без ЭЦП существовать не может. Если ЭЦП не применяется, то можно говорить лишь об электронном образе документа и не более того. Никакие графические образы подписи на документе (например, отсканированный бумажный оригинал) не могут рассматриваться как аналог собственноручной подписи. Более того, подобная практика вредна, поскольку создает иллюзию защищенности системы и ее участников;

важно понимать, что ЭЦП не обеспечивает конфиденциальность электронного документа. Эту задачу решает шифрование, которое, в свою очередь, никакого отношения к обеспечению юридической значимости документа не имеет. В случае совместного использования ЭЦП и шифрования нужно учитывать, что для того, чтобы ЭЦП была юридически значимой, пользователь должен видеть и понимать, чтó он подписывает. Поэтому необходимо вначале создать ЭЦП, а уж затем зашифровать документ, который перед проверкой подписи должен быть расшифрован;

с определенностью можно констатировать, что на сегодняшний день нормативно-правовая и техническая база для реализации юридически

значимого электронного документооборота в масштабах государства в нашей стране еще не создана. Тем не менее даже в рамках имеющегося законодательства и технической базы можно реализовать внутренний юридически значимый электронный документооборот в работе отдельно взятой организации или нескольких компаний, входящих в одну структуру, — корпоративный электронный документооборот.



Начиная работать с ЭЦП, пользователь делает запрос средствами СЭД на получение ключевой пары (а); затем запрашивает сертификат для только что сгенерированного открытого ключа (б); при необходимости подписать документ (только что созданный или полученный из СЭД) его данные передаются в криптопровайдер для генерации ЭЦП, после чего на ЭЦП ставится штамп времени (в); после получения документа из СЭД получатель передает его для проверки в криптопровайдер, где проверяется не только сама ЭЦП, но также сертификат и штамп времени (г)

Уже сегодня многие внутренние документы организации можно перевести в электронный вид (например, служебные записки, заявки на выделение денежных средств, различные внутренние отчеты, поручения и т. п.). Необходимо разработать нормативно-правовую базу организации, регламентирующую применение ЭЦП. Такой регламент обеспечит электронным документам юридическую силу — возможность представлять их в суде в качестве доказательства. Безусловно, небольшая правоприменительная

практика вносит некоторые ограничения в применение ЭЦП, но не является принципиальным барьером для построения в отдельной компании внутреннего юридически значимого электронного документооборота.

Действующие лица и исполнители

Как следует из вышеизложенного, ЭЦП — это аналог собственноручной подписи человека, применяемый в электронных документах. Электронно-цифровая подпись создается с помощью закрытого ключа — уникальной последовательности символов, которая известна его владельцу и предназначена для создания ЭЦП в электронных документах с использованием соответствующих средств.

Получатели электронного документа, подписанного ЭЦП, имеют возможность проверить действительность подписи посредством открытого ключа и убедиться в том, что документ подлинный, а ЭЦП принадлежит именно тому лицу, которое в нем указано. Открытый ключ — это уникальная последовательность символов, которая математически связана с закрытым ключом ЭЦП. Открытый и закрытый ключи образуют так называемую ключевую пару.

Открытый ключ доступен любому пользователю информационной системы в составе сертификата ключа. Сертификат ключа является аналогом документа, удостоверяющего личность (например, паспорта). Это документ на бумажном носителе либо электронный документ с ЭЦП уполномоченного лица (сотрудника) удостоверяющего центра. Сертификат ключа помимо открытого ключа ЭЦП содержит идентификационные данные владельца. Сертификат передается пользователю СЭД и выполняет две задачи: подтверждает подлинность ЭЦП и идентифицирует владельца сертификата ключа подписи.

И в том и в другом случае используются средства электронно-цифровой подписи — программно-аппаратный комплекс, обеспечивающий реализацию хотя бы одной из следующих функций: создание ЭЦП в электронном документе с использованием закрытого ключа ЭЦП; подтверждение с использованием открытого ключа ЭЦП подлинности ЭЦП в электронном документе; создание закрытых и открытых ключей ЭЦП.

Аналогом третейского судьи, которому доверяют все участники документооборота, является **удостоверяющий центр** — организационная структура, осуществляющая деятельность по управлению сертификатами ключей и поддержке их использования в различных подсистемах корпоративной информационной системы. Удостоверяющий центр может быть внешней организацией или подразделением той или иной компании.

Еще один участник процесса — криптопровайдер. Это программный или аппаратно-программный модуль, реализующий один или несколько криптографических алгоритмов и предоставляющий свои функции внешним системам.

Аналогом даты на бумажном документе, которую собственноручно проставляет лицо, подписывающее документ, является штамп времени. Речь идет о свидетельстве третьей доверенной стороны — организационной единицы, носящей название службы штампов времени. СЭД передает туда так называемое хеш-сообщение, которое получается в результате криптографического преобразования документа. На это сообщение служба ставит штамп (средствами своего программно-аппаратного обеспечения), удостоверяющий, что электронный документ существовал на данный момент времени. В результате к хеш-сообщению добавляется значение, указывающее, когда службой штампов времени был получен запрос на проставление штампа времени. Проставляемое значение служба штампов времени подписывает собственной ЭЦП и возвращает документ обратно в СЭД.

Совокупность аппаратно-программного обеспечения, а также персонала, политик и процедур, необходимых для создания, хранения, распределения, управления жизненным циклом и использования сертификатов открытых и связанных закрытых ключей называется инфраструктурой открытых ключей (ИОК).

Как всегда, все дело в деталях реализации!

Выбирая СЭД с поддержкой ЭЦП, следует обратить внимание на особенности реализации выбранной системы. Рассмотрим ключевые аспекты, которые необходимо учитывать.

Не только содержание, но и форма

Во многих СЭД в качестве электронного документа рассматривается файл какого-либо типа (например, Microsoft Word или Adobe Acrobat), прилагаемый к регистрационной карточке. Хотелось бы обратить внимание на одно обстоятельство: подписание просто файлов (содержательной части документов) не представляет большого интереса для организации. Строго говоря, не вся информация в документе является “неструктурированной”, документ кроме содержательной части содержит реквизиты, которые можно и нужно выделять в отдельную структуру, чтобы в дальнейшем осуществлять по ним поиск и классификацию документов. Во многих ситуациях полезно подписывать не только содержание, но и форму. В этом случае можно отображать на экране компьютера и распечатывать электронный документ в том виде, в котором он был подписан, что позволит избежать всяческих конфликтных ситуаций.

Все нюансы бумажного документооборота

ЭЦП должна быть равнозначна собственноручной подписи и учитывать все нюансы бумажного делопроизводства. А именно — необходимо, чтобы СЭД позволяла подписать часть документа, поставить подпись в электронном документе последовательно (подписывается документ и все имеющиеся ЭЦП), параллельно (подписывается документ и все ЭЦП нижележащих уровней).

На рисунке 3 приведены примеры использования ЭЦП в документе. Подпись “заверяю” — последовательная подпись первого уровня — охватывает только

содержательную часть документа (это подпись автора документа). Подписи “согласовано 1” и “согласовано 2” (визы согласующих) — это параллельные подписи второго уровня. Они охватывают содержательную часть документа и подпись первого уровня и при этом не зависят друг от друга. Подпись “утверждаю” (виза руководителя) — последовательная подпись третьего уровня — охватывает содержательную часть документа и все предыдущие подписи.

Формат электронного документа

Для полноценной реализации ЭЦП система электронного документооборота должна поддерживать формат документа, являющийся канонической формой, к которой будет приводиться любой “электронный документ” в СЭД. С точки зрения удобства работы и перспективы развития и интеграции предпочтительны СЭД, которые для описания формата документа используют язык XML. В настоящий момент международными организациями ведется работа по созданию стандарта формата электронного документа.

Штамп времени

Важно отметить, что при работе с ЭЦП неизбежно возникает проблема, обусловленная тем, что срок действия любого сертификата ограничен определенным промежутком времени. По истечении срока действия сертификата все созданные при его помощи ЭЦП теряют свое значение, поскольку невозможно определить, была ли ЭЦП создана, когда сертификат еще действовал или когда срок его действия уже закончился. А это, в соответствии с федеральным законом “Об электронной цифровой подписи”, автоматически означает недействительность ЭЦП.

Поэтому внимание заслуживают лишь СЭД, интегрированные со службой штампов времени, которая позволяет в один из атрибутов системы помещать штамп, фиксирующий момент создания ЭЦП. При таком решении имеется возможность проверять ЭЦП с учетом того, действовал ли сертификат в момент создания этой ЭЦП, а не в момент проверки.

Архивная копия электронного документа

СЭД должна позволять участнику системы получить архивную копию подписанного электронного документа, которая может быть представлена в качестве доказательства в случае возникновения конфликтной ситуации. Разумеется, необходимо учитывать ограничения политики безопасности, касающиеся конфиденциальных документов.

Создание ЭЦП под документом

Это действие должно выполняться пользователем осознанно. Не допускается подписывать документ в автоматическом режиме. Система обязательно должна задать вопрос, будет ли пользователь подписывать документ. Во многих существующих СЭД этому не уделяется должное внимание. Более того, некоторые разработчики, увлекаясь автоматизацией, специально реализуют автоматическую простановку ЭЦП под документом, что является абсолютно неверным подходом.

Делегирование полномочий

Отдельный вопрос — делегирование должностных полномочий одного пользователя системы другому. Очень часто руководители передают свое право подписания электронного документа доверенному лицу, при этом параллельно подписывают бумажный экземпляр документа, который в данном случае и является оригиналом. Вопрос не простой. Следует получить квалифицированную консультацию у юриста, в каких случаях делегирование допустимо и не противоречит действующему законодательству и каким образом этот факт должен быть оформлен документально. Просто передавать другому сотруднику свой закрытый ключ для создания ЭЦП недопустимо, поскольку такая ситуация трактуется как компрометация ключа, а следовательно, полученная под документом ЭЦП не является легитимной.

Если говорить о реализации СЭД, то технически делегирование реализуется как выпуск удостоверяющим центром специальных сертификатов, имеющих ограниченное применение (указывается в сведениях об отношениях) и срок действия; при этом в реквизитах ЭЦП указывается, от кого делегированы данные полномочия. Для многих читателей термин “сведения об отношениях” почти наверняка покажется странным. Этим термином обозначается свойство сертификата, позволяющее ограничить область его применения. Например, сотрудник имеет право поставить подпись под служебной запиской, но не имеет права подписать финансовый документ.

“Свои” или “чужие”?

При развертывании в организации СЭД с ЭЦП необходимо решить, какую инфраструктуру открытого ключа использовать: разворачивать ли собственную (внутренняя) или прибегнуть к услугам сторонней компании (внешняя).

Как правило, крупные компании и холдинги реализуют ИОК собственными силами, т. е. службы являются внутренними. Для средних организаций экономически целесообразным может оказаться использование услуг других компаний. При этом между организацией и компанией-поставщиком заключается договор на предоставление услуг удостоверяющего центра и службы штампов времени.

Заключение

Изначально СЭД проектировались без учета применения ЭЦП, они моделировали работу с бумажными документами, от которых организации не собирались отказываться. По мере осознания того, что ЭЦП использовать нужно, разработчики стали встраивать в существующие СЭД функции ЭЦП, рассматривая их как дополнительные. Однако в результате получались решения с ограниченными возможностями, поскольку полноценное встраивание ЭЦП требовало слишком больших переделок в существующих системах.

Сегодня, на очередном витке развития информационных технологий, разработчики вновь создаваемых СЭД уже не рассматривают ЭЦП как некое дополнение и учитывают необходимость ее применения уже на этапе разработки архитектуры системы.

Мировой опыт развития СЭД показывает, что перспективы применения ЭЦП в электронном документообороте и смежных областях весьма впечатляющи. Наблюдается бурное развитие технологий потокового сканирования и распознавания графических образов, что позволяет перевести практически любые бумажные документы в электронный вид и обеспечить эффективный полнотекстовый поиск по ним. Развивается ИОК. В сочетании с общей тенденцией к ускорению принятия решений по документам и потребностью именно в юридически значимых электронных документах это приводит к тому, что электронная цифровая подпись становится востребованной как никогда ранее.

Статья взята из журнала PCWeek/RE, №34/2006

Полную версию статьи можно прочитать по адресу: http://www.pcweek.ru/?ID=615661

Информация Национального удостоверяющего центра.

Издаваемые Национальным удостоверяющим центром Сертификаты ключей подписи, оказываемые услуги, включая развертывание у заказчика системы электронного документооборота и электронных торговых площадок, созданных нашими партнерами, использование электронных цифровых подписей в корпоративной информационной системе «ТПП-СОЮЗ» (**С**истеме **О**бмена **Ю**ридически **З**начимой информацией Торгово-промышленной палаты России) полностью соответствуют требованиям, изложенным в настоящей статье, положениям федерального закона «Об электронной цифровой подписи» и других нормативных документов, регламентирующих данную сферу деятельности.