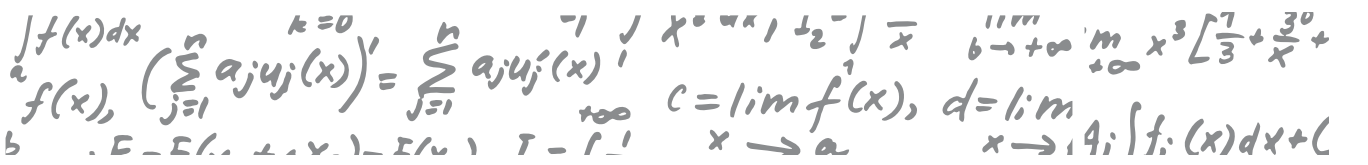
В ногу со временем

Мой папа математик, а не юрист



Желание написать статью об электронных подписях появилось у меня достаточно давно. Тема важная, интересует многих. Но, несмотря на регулярное проведение консультаций пользователей и партнеров по этому вопросу, перенести свои знания на бумагу все как-то не получалось.

После принятия закона Российской Федерации от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи" я было задумал написать полемическую статью о его качестве и применимости в корпоративном документообороте. Основные претензии к этому закону заключались в том, что он не рассчитан на применение в корпоративных и открытых информационных системах, не учитывает растущие потребности взаимодействия с субъектами иностранных государств и физическими лицами.

Но спустя некоторое время я остудил свой пыл, убедившись, что на отдельной части правового пространства закон все-таки работает. Да, конечно, он не оперирует вышеописанными понятиями. Значит – это просто другой закон. В конце концов, есть Гражданский кодекс, который, хоть и не без некоторого расширенного толкования, регулирует правовые нормы при работе с электронными подписями, не попавшими под строгую букву закона об ЭЦП. А писать о юридических тонкостях и судебной практике – явно не мой конек.

Прогнозируемая неожиданность

Время шло своим чередом, и мы подготовили к выходу новую, четвертую версию TDMS. Изменения коснулись и работы с подписями. Несмотря на то, что электронные подписи были введены еще в третьей версии, разработчики конфигураций на платформе TDMS неохотно их использовали из-за достаточно жесткого поведения системы при работе с ними. Информационный объект мог быть подписан только полностью, а любое изменение его свойств приводило к тому, что все подписи "под ним" становились недействительными. Кроме того, пользователями высказывались пожелания о более гибкой обработке событий при работе с подписями.

В результате в TDMS 4.0 были внесены следующие дополнения к свойствам подписей:

- добавлена визуальная настройка подписываемых свойств. При создании новой подписи производится выбор свойств, которые будут подписываться и, как следствие, влиять на статус подписи при изменении информационного объекта;
- появились новые программные обработчики событий и методы работы с подписями;
- добавлена возможность применения пользователями при работе с подписями TDMS персональных электронных сертификатов, в качестве которых могут использоваться сертификаты, полученные как из корпоративных хранилищ, так и в удостоверяющих центрах, обладающих лицензиями в соответствии законом Российской Федерации от 10 января 2002 г. № 1-ФЗ "Об электронной цифровой подписи";
- упрощен интерфейс пользователя, используемый при работе с подписями.

Это были запланированные и продуманные действия, основанные на потребностях и пожеланиях пользователей. И вряд ли только на их основе я или кто-то из моих коллег взялся бы писать статью. Но тут случилось хоть и прогнозируемое, но при этом достаточно неожиданное событие, которое заставило-таки "взяться за перо": 30 марта 2011 года был принят новый закон об электронной подписи. Событие "прогнозируемое", потому что новый закон активно обсуждался, и было понятно, что его скорее примут, чем нет. "Неожиданное", поскольку еще в конце февраля 2011 года после ознакомления с проектом документа у меня сложилось ощущение, что он пока далек от совершенства и, несмотря на статус "принят во втором чтении", будет еще серьезно дорабатываться. Но, как стало ясно уже через месяц, я ошибся.

В соответствии с законом

Разработка нового документа в первую очередь была мотивирована тем, что положения закона 2002 года не соответствовали принципам регулирования электронных подписей, действующим в европейских государствах. По сути, новый закон не отменил старый, а стал шире толковать электронную подпись, тем самым значительно расширив возможности для ее применения.

До принятия нового закона "юридически значимым" признавался только один вид электронной подписи, что вызывало много споров на тему, что делать с другими видами. Получалось как в известном анекдоте, когда "часть тела" есть, а слова нет. Рассуждения на тему электронной подписи породили ряд многозначительных и плохо понимаемых терминов, таких как "юридически значимый документооборот"[1].

Закон вводит три типа электронной подписи: простую, усиленную и квалифицированную. Это наш российский аналог европейским *Electronic Signature*, *Advanced Electronic Signature* и *Qualified Electronic Signature*.

Простая подпись служит для подтверждения факта формирования подписи определенным лицом. Чтобы установить простую подпись, пользователь должен себя идентифицировать любым из доступных способов. Например, входя на личную страницу сайта бронирования авиабилетов, он вводит свои логин и пароль. В дальнейшем информация о выполненных

[1] "Юридически значимым" документооборот становится не от того, какой тип информационной системы используется, и даже не от положений, на основании которых данная система применяется. Юридически значимый документооборот – это обмен юридически значимыми документами. Закон, который может сделать документооборот юридически значимым, – это закон об электронном обмене документами.

пользователем действиях (например, подтверждение согласия с выписанным ему счетом) будет храниться в базе данных данного сайта.

Большинство информационных систем обладают возможностью создавать простые подписи, иногда даже не называя их "электронными подписями". В системах, построенных на платформе TDMS 3.0, модуль согласования и утверждения проектной документации, равно как и модуль управления потоками работ (передачи заданий), использует принцип применения простой электронной подписи. Для признания подобных электронных подписей юридически значимыми в организациях, применяющих данные модули, установлены правила работы с подписями, принята их юридическая сила и определена степень ответственности пользователей системы.

Усиленными называют подписи, полученные в результате *криптографического преобразования* информации с использованием ключа подписи. Данный вид подписи позволяет не только определить лицо, подписавшее электронный документ, но и обнаружить факт внесения изменений в электронный документ после его подписания.

Усиленные подписи TDMS 4.0 могут быть сформированы тремя способами. Первый унаследован от TDMS 3.0. Он использует в качестве ключа подписи уникальные идентификационные данные о пользователе, хранящиеся в системе с момента его регистрации. Чтобы установить подпись, пользователь должен ввести для нее персональный пароль.

Второй способ, появившийся в TDMS 4.0, использует в качестве ключа подписи персональный сертификат пользователя. Для создания корпоративного хранилища сертификатов рекомендуется использовать встроенные в современные серверные ОС Windows службы сертификатов Active Directory. Эти службы предоставляют настраиваемые услуги выдачи сертификатов открытого ключа, используемых в соответствующих программных системах, и управления этими сертификатами.

Третий способ формирования электронной подписи также стал доступен только в новой TDMS 4.0. Он использует в качестве ключа подписи *квалифицированный сертификат*, полученный из аккредитованного удостоверяющего центра. Чтобы создать и проверить такую электронной подпись, используются средства, получившие подтверждение соответствия требованиям, установленным в соответствии с новым Федеральным законом об электронной подписи[2].

Формирование и проверка электронной подписи третьим способом соответствует закрепленному в новом законе определению *усиленной квалифицированной* электронной подписи, в то время как первые два способа – определению *усиленной неквалифицированной* электронной подписи.

Следует отметить, что усиленная квалифицированная (или просто "квалифицированная") электронная подпись является прямым наследником электронной цифровой подписи, определенной в законе 2002 года. Поэтому и сфера ее применения остается практически неизменной. Квалифицированная подпись используется для обеспечения взаимодействия с государственными организациями.

Нас же, конечно, больше интересует применение нового типа подписи, а именно усиленной неквалифицированной (или просто "усиленной") электронной подписи. Насколько оправданно ее использование в корпоративной информационной системе? Есть ли преимущества у данного типа подписи перед простой подписью?

Как и в законе 2002 года, действующее законодательство не регламентирует применение того или иного вида электронной подписи в рамках корпоративных систем. Чтобы электронная подпись получила юридическую силу, владелец информационной системы должен выступить с собственной законодательной инициативой и ввести регламент работы с электронными документами. Если регламент содержит описание того, какие действия пользователя системы приравниваются к собственноручной подписи, такие действия будут иметь юридическую силу.

Используемое в усиленной подписи криптографическое преобразование позволяет зафиксировать состояние подписанного содержимого. По сравнению с простой подписью это дает два фундаментальных преимущества:

- подделать новый вид усиленной подписи TDMS, даже обладая правами системного администратора TDMS, крайне затруднительно. Для этого необходимо обладать закрытым ключом пользователя;
- в случае изменения подписанного содержимого подпись автоматически станет недействительной.

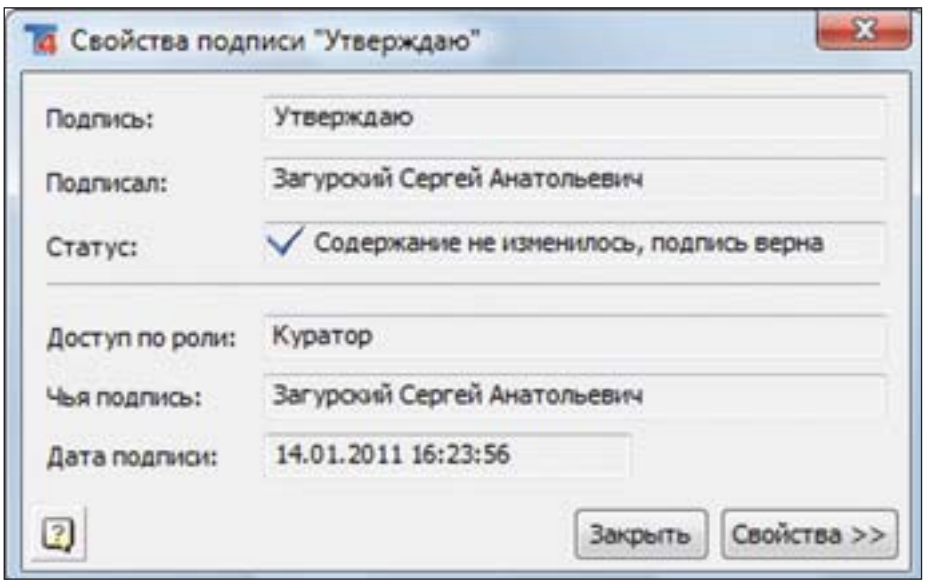


Рис. 1. Свойства подписи

Обновленные подписи

Следует понимать, что подписи TDMS являются аналогами собственноручной подписи и в первую очередь служат для применения в рамках внутреннего документооборота. Именно этим обусловлены такие их особенности, как возможность установить несколько подписей на один документ и типизация подписей. Типы (шаблоны) подписей TDMS позволяют определить наименование подписи (например, "Начальник отдела", "Разработал", "Утверждаю" и т.п.) и требуемые права на установку подписи.

С точки зрения пользователя, процесс подписания достаточно прост. Завершив

[2]Для работы с квалифицированными подписями необходимо приобретение сертифицированного средства криптографической защиты информации российского производства.

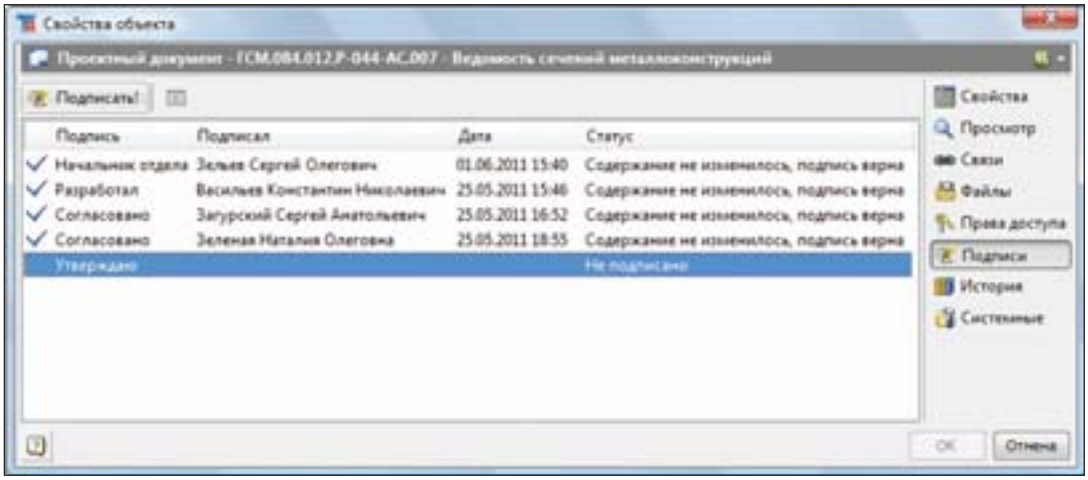


Рис. 2. Список подписей документа

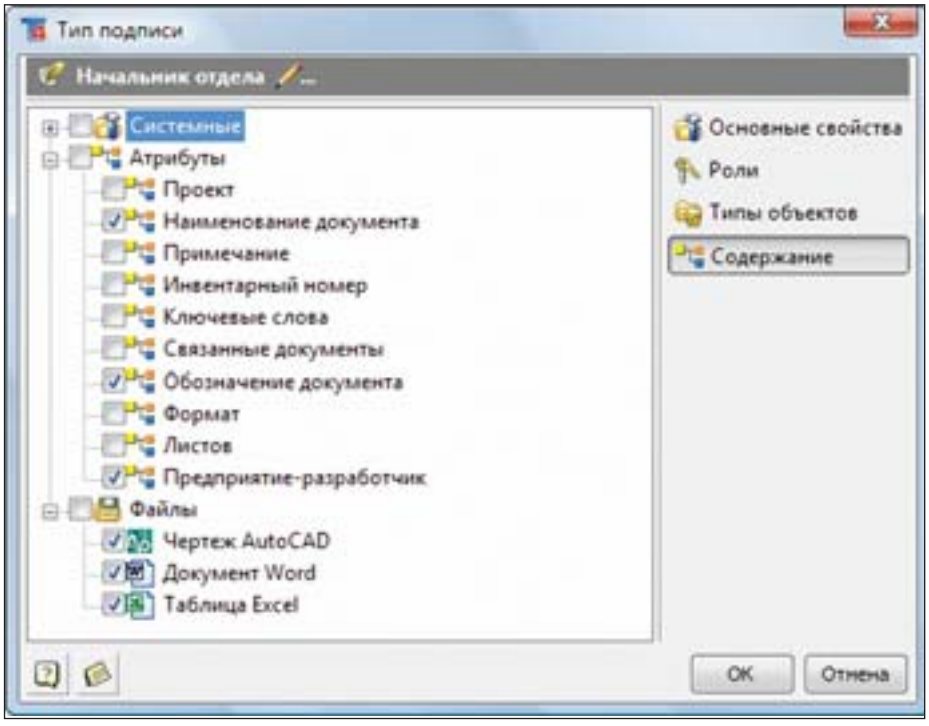


Рис. 3. Настройка подписываемого содержимого в шаблоне подписи

свою часть работы над документом, пользователь выполняет команду *Подписать*. В зависимости от служебных обязанностей пользователя будет использован определенный вид подписи. Устанавливая подпись, пользователь создает реквизит документа, который формируется из персонального закрытого ключа пользователя, подписываемого содержимого, времени подписания и ряда других свойств подписи (рис. 1).

Чтобы проверить подписи на документе, пользователю необходимо перейти на вкладку *Подписи* диалога свойств документа (рис. 2). Если информация в документе не менялась, и установлена подлинность сертификата, с помощью которого была создана подпись, в свойствах подписи будет присутствовать фраза "Содержание не изменилось, подпись верна". В том случае если, например, документ был модифицирован, статус подписи изменится на "Содержание изменилось, подпись отозвана".

Важнейшим отличием обновленной системы работы с подписями в TDMS 4.0 стала возможность настройки подписываемого содержимого документа в шаблоне подписи. Проще говоря, при подготовке системы к эксплуатации ее разработчик может указать, какие именно свойства документа должны быть защищены подписью от изменений, а какие нет (рис. 3).

Такой подход позволяет изменять определенные свойства документа даже после того, как он был подписан. Например, если инвентарный номер присваивается уже после согласования и утверждения документа, действие по его установке может привести к изменению статуса подписи. Однако если инвентарный номер не является подписываемым свойством, его изменение никак не повлияет на ранее установленные подписи.

TDMS API – ключ к неограниченным возможностям

Для еще более гибкого управления процессом использования подписей в документообороте организации в TDMS были расширены программные возможности работы с ними. К таким возможностям относятся новые свойства подписи, обработчики событий и методы. Теперь TDMS API в общей сложности содержит более 40 свойств, методов и обработчиков событий для работы с подписями.

Дополнительно, если вы захотите добавить функции создания и проверки электронной подписи с помощью сторонних алгоритмов, отображения информации об электронной подписи и сертификате, шифрования и расшифровки данных, вы можете подключить компоненту CAPICOM. Эта компонента обеспечивает доступ через технологию COM к реализованным в CryptoAPI криптографическим функциям, делая их доступными в среде программирования TDMS.

К сожалению, объем журнальной публикации не позволяет привести примеры программного кода, которые могут быть использованы для гибкой настройки процессов подписания документов. Поэтому я приглашаю вас к прочтению второй части этой статьи, написанной мной в соавторстве с одним из разработчиков платформы TDMS, Алексеем Мызниковым, на нашу "электронную площадку". На обновленном сайте *www.tdms.ru* приведены примеры работы с усиленными подписями, в том числе – с возможностью подключения сторонних алгоритмов формирования подписей с использованием CAPICOM.

Кроме того, во второй части статьи подробно освещаются принципы работы подписей TDMS 4.0, а также предлагаются программные решения для управления процессами установки и отзыва подписей. В качестве примеров рассматриваются задачи установки одной подписи поверх другой и автоматического сброса всех последующих подписей в случае отзыва одной из предыдущих.

Сергей Загурский
E-mail: serge@csoft.ru