**Как подписывать с помощью ЭЦП электронные документы различных форм**

Юрий Маслов

При создании и внедрении систем электронного документооборота неизбежно встает задача определения электронного документа и его подписи. Мы уже почти привыкли работать с электронной цифровой подписью (ЭЦП) для файлов, но иногда наши документы представляют собой файлы определенного формата или вообще не являются файлами.

В настоящей статье рассмотрим несколько наиболее распространенных вариантов работы с ЭЦП для электронных документов определенных форматов.

**Подпись в HTML-форме**

Такая задача возникает при встраивании средств ЭЦП в системах с "тонким" клиентом, когда пользователь работает в системе через Web-браузер (MS IE). В таких системах поступают следующим образом: создается скрытое hidden-поле в форме. Когда пользователь нажимает кнопку типа "подписать и отправить", соответствующий скрипт обработчика (например, на VBScript) формирует строковую переменную, в которую методом конкатенации записывают важную информацию по идентификации документа и содержимое текстовых полей, которые ввел пользователь. Далее сформированная строковая переменная подписывается. Чаще всего используются методы объектов CAPICOM.dll, неотделенная подпись. Подписанная строковая переменная и есть электронный документ. Подписанный документ (подписанная строка) записывается в hidden-поле и методом POST передается на сервер. Серверное приложение проверяет подпись в переменной, полученной из hidden-поля, и в зависимости от результатов проверки ЭЦП и содержательной части электронного документа осуществляет его дальнейшую обработку. Важным моментом является сохранение подписанного документа на сервере. Для этого, как правило, создают таблицу в базе данных системы с двумя полями: поле ключа и строковое поле, содержащее подписанный электронный документ.

**Подпись в базе данных**

Довольно часто встречается нефайловая, или строковая, форма представления электронного документа, а электронный документ – как совокупность записей в таблицах базы данных. Для подписания такого документа значения полей записей в таблицах базы данных приводятся в строковый тип, и с помощью конкатенации формируется строковая переменная, отражающая существенную содержательную и идентификационную часть документа. Именно эта строка теперь считается оригиналом электронного документа и подписывается. Подписанная строка сохраняется в соответствующей таблице базы данных системы с двумя полями: поле ключа документа и строковое поле, содержащее подписанный электронный документ.

**Подпись документов в формате XML**

Если документ представлен в формате XML, то имеется несколько подходов к формированию его подписей: формирование ЭЦП XML-документов XMLdsig для Windows (MSXML5, MSXML6) с использованием Microsoft Office InfoPath 2003 – новой составляющей системы Microsoft Office; подпись XML-документа как обычного файла. Иногда для подписи в XML-документе в тэге документа создают отдельный атрибут, в который заносится ЭЦП от символьной строки переменной длины, содержащей значения атрибутов тэга документа. Такой достаточно интересный подход к подписи XML-документа также встречается, и он является вполне легитимным.

**Подпись файлов в формате PDF**

Для формирования и проверки ЭЦП и обеспечения юридической значимости электронных документов, формируемых в формате PDF, компания "КРИПТО-ПРО" разработала специальный продукт, называемый "КриптоПро PDF". Он является модулем создания и проверки ЭЦП и предназначен для формирования и проверки ЭЦП в программax Adobe Reader, Adobe Acrobat версии 7 и выше. "КриптоПро PDF" разработан с использованием программного интерфейса Adobe Systems Inc. и заверен электронной цифровой подписью компании Adobe Systems.

Это позволяет использовать сертифицированные средства криптографической защиты информации "КриптоПро CSP" в продуктах Adobe Acrobat, Adobe Reader и Adobe LiveCycle ES. Важное замечание: "Крипто-Про CSP" для проверки ЭЦП не требует активации лицензии, то есть работает бесплатно. Достаточно просто установить этот продукт и проверять подпись с использованием Adobe Reader.

**Подпись многофайловых документов**

Иногда документ может представлять собой достаточно большую совокупность файлов. Например, сведения о первичных документах для совершения операций в реестре владельцев инвестиционных паев паевого фонда, полученных от управляющей компании. В этом случае можно формировать для каждого документа свою ЭЦП, а можно от этого отказаться. Если по каким-либо причинам формирование ЭЦП для каждого файла документа невозможно, то создают еще один файл текстового формата, в который записывают идентификационные данные документа и значения хэш-функций для каждого файла документа. Именно этот файл (карточка документа) и подписывают. Но в данном случае в системе должен быть предусмотрен инструмент для пользователя, позволяющий рассчитать значения хэш-функций для каждого файла и сравнения вычисленных значений с данными карточки документа.

Юрий Маслов, коммерческий директор ООО "КРИПТО-ПРО"

**Список литературы**

Information Security №1, февраль-март 2009