ЭЦП и шифрование в системах электронного документооборота

Публикация продолжает тему шифрования данных при хранении применительно к системам электронного документооборота (СЭД) и, в частности, к DocsVision. В качестве важного дополнения к технологиям шифрования при хранении рассматривается использование электронной цифровой подписи (ЭЦП), позволяющей в значительной степени обеспечить защиту целостности информации.

Шифрование и ЭЦП – два базовых механизма защиты информации в СЭД DocsVision

Защиту данных криптографическими методами принято классифицировать по месту применения шифрования:

- уровень приложения;
- уровень файловой системы;
- сетевой уровень;
- уровень устройства.

Защита на уровне приложения оптимальна в том смысле, что на уровне приложений исходно формулируется ценность данных и риски, связанные с нарушением информационной безопасности.

Несмотря на то, что с общей точки зрения сервер базы данных может рассматриваться как приложение по отношению к операционной системе, как правило, бизнес-логика находится выше, не только выше таблиц и столбцов, но и выше пользовательских схем.

Системы электронного документооборота – хороший пример.

Как правило, документ как файл существует в паре со своей электронной регистрационной карточкой. В процессе обработки документа к нему присоединяется еще ряд объектов – резолюции, связанные с ними задания, согласования и утверждения.

В таком контексте управленческий документ – зафиксированная история возникновения, обработки и принятия решений по управленческому событию. Полномочия на принятие решений являются важнейшим ресурсом предприятия и должны контролироваться соответствующим образом.

Для осознания задачи надо также иметь в виду единство целей информационной безопасности, определяемое в виде триады:

- целостность;
- конфиденциальность;
- доступность.

Электронная цифровая подпись попадает в основном в цели защиты целостности, а шифрование – в цели защиты конфиденциальности. Это различие надо иметь в виду, несмотря на общую для этих задач технологическую базу – архитектуру открытых ключей.

Электронная цифровая подпись – это механизм защиты сообщения, файла или целостного набора данных, предназначенный для решения трех задач:

1) удостоверение источника сообщения. В зависимости от деталей определения документа могут быть подписаны такие поля, как “автор”, “внесенные изменения”, “метка времени” и т. д.;

2) защиту от изменений сообщения. При любом случайном или преднамеренном изменении документа (или подписи), подпись станет недействительной;

3) невозможность отказа от авторства. Так как создать корректную подпись можно, зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под сообщением.

Набор данных как целостный объект определяется всегда на уровне приложения, файл – на уровне файловой системы, письмо – на уровне приложения электронной почты, документ – на уровне системы управления документами.

Технологическая база защиты информации в СЭД

Службы инфраструктуры открытых ключей PKI – внешние по отношению к СЭД, поэтому настройки DocsVision сводятся к установлению связей между системой (вернее, ее криптоклиентом,

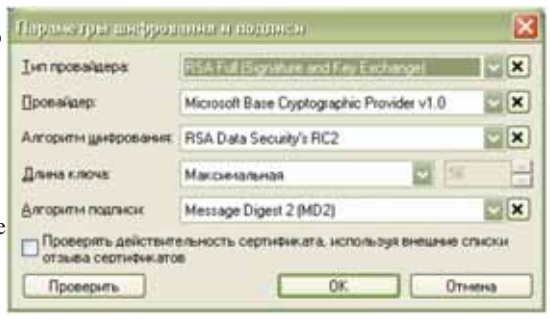

Рис. 1. Настройка параметров шифрования и ЭЦП в СЭД DocsVision.

компонентой, взаимодействующей с инфраструктурой PKI) и этими внешними службами.

В области настроек имеется карточка "Настройки делопроизводства". В разделе "Шифрование" необходимо выбрать один из установленных в системе криптопровайдеров и указать параметры его настройки, например, алгоритм шифрования, длину ключа и алгоритм подписи (рис. 1).

Настроив связи с инфраструктурой PKI, можно использовать электронную подпись и шифровать файлы, хранящиеся в системе.

Подписать или зашифровать файл можно, нажав кнопку "Подписи и шифрование" в карточке документа.

Кроме Microsoft Crypto API, DocsVision поддерживает PGP.

Поскольку службы ЭЦП и шифрования являются внешними по отношению к системе, то технически все это работает одинаково надежно в любой СЭД, но у криптоклиента DocsVision имеются преимущества в интеграции, обеспечивающие удобство настройки и использования электронной подписи.

Этих преимуществ два:

- синхронизация сертификатов между сервером сертификатов и DocsVision (рис. 2) через службу каталогов Active Directory (когда и каким образом происходит синхронизация сертификатов);

Рис. 2. У криптоклиента DocsVision есть возможность синхронизации сертификатов между сервером сертификатов и DocsVision через службу каталогов Active Directory.

- возможность использования любой PKI-инфраструктуры, базирующейся на Microsoft CryptoAPI, в том числе входящей в состав Windows, и в этом смысле бесплатного криптопровайдера Microsoft, или криптопровайдера КриптоПро CSP 3.0, имеющего сертификат соответствия ФСБ на использование для формирования ключей шифрования и ключей электронной цифровой подписи, шифрования и имитозащиты данных, обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну.

Базовые средства платформы DocsVision позволяют подписывать и шифровать хранящиеся в системе файлы. Однако, как мы уже говорили, задача поддержания целостности документа не исчерпывается защитой файла, нужно защищать также резолюции, согласования и утверждения.

В приложении DocsVision "Административное делопроизводство" реализована возможность подписывания не только файла, но и факта регистрации документа, визы на документе и утверждающей подписи на проекте резолюции (рис. 3).

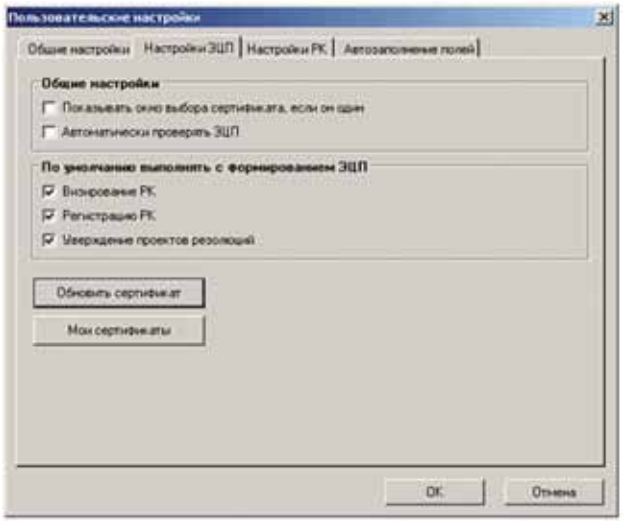

Рис. 3. В DocsVision в опции "Административное делопроизводство" реализована возможность подписывания не только файла, но и факта регистрации документа, визы на документе и утверждающей подписи на проекте резолюции.

Если включена автоматическая проверка ЭЦП, то она будет производиться при открытии регистрационной карточки, при переходе к общим параметрам карточки, заполняемым при регистрации, при открытии карточек заданий, для которых сформирована ЭЦП.

Говоря о защите файлов, следует сказать о защите операций с ними, выполняемых в связанном с файлом приложении (печать, копирование фрагмента, сохранение на локальной рабочей станции). Такие операции, в принципе, можно защитить только на уровне приложения. Для этого приложение должно поддерживать соответствующие механизмы. В частности, файлы Microsoft Office эффективно защищаются с помощью технологии Information Rights Management (IRM), встроенной в приложения Office и использующей службу Rights Management Service, входящую в Microsoft Windows Server. Используя RMS, пользователи, работающие с информацией, могут указывать тех, кому разрешено использовать файл. Также они могут определять действия, которые разрешено производить с файлом. Например, они могут предоставить права на открытие, внесение изменений, печать, пересылку документа и т.п. Технология IRM поддерживает создание пользовательских шаблонов политик использования файлов. В случае применения IRM права на использование информации всегда сохраняются вместе с ней даже в том случае, если эта информация используется за пределами сети. Это означает, что права на использование будут применяться к защищенной информации даже в том случае, если сотрудник открывает сообщение электронной почты или документ автономно, или когда он предварительно сохранил его на диске. В основе RMS-IRM технологии лежит та же самая PKI-инфраструктура, расширенная до операций с файлом, определяемых в контексте приложения.

Следует отметить, что при использовании инфраструктуры PKI шифрование/дешифрование происходит в месте создания или использования документа (на рабочей станции пользователя). Шифрование документа в месте хранения (в базах данных или на защищенных файловых серверах) производится на сервере, причем делать его необходимо "на лету", что сильно увеличивает нагрузку на сервер и, соответственно, его цену.

Основные связи администраторов, пользователей, приложений и основных компонент инфраструктуры шифрования и электронной подписи даны на рис. 4.

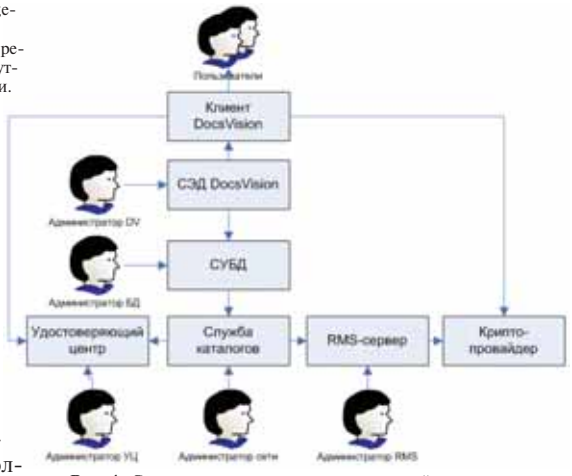

Рис. 4. Связи администраторов, пользователей, приложений и основных компонент инфраструктуры шифрования и электронной подписи.

Выводы

1. Эффективная защита целостности управленческой информации может быть реализована только на уровне приложения.

2. Кроме защиты файла документа, необходимо защищать подписью действия,

выполненные с этим документом различными пользователями.

3. Система DocsVision поддерживает защиту целостности цифровой подписью и конфиденциальности – шифрованием с использованием криптопровайдеров, совместимых с Microsoft Crypto API или PGP версии 6.5.8.

4. ЭЦП и шифрование – разные функции, построенные на общей технологии PKI.

5. Надежность подписи и шифрования определяются доверием к издателю сертификата ключей – удостоверяющему центру.

6. Для дифференциальной защиты файла документа по отношению к различным операциям, которые пользователь может выполнить с ним в приложении, необходимо использовать встроенные в приложение механизмы, например, технологии RMS-IRM для документов Microsoft Office.

7. Для усиления надежности защиты необходимо прибегать к услугам внешнего удостоверяющего центра, либо административно разделять функции администрирования инфраструктурой, базой данных и приложением.

Описанные механизмы успешно применяются в ряде крупных внедрений системы DocsVision, в частности, в проектах Министерства экономического развития и торговли РФ, Министерства природных ресурсов РФ, Самарской Губернской Думы.

Сергей Курьянов,
директор по развитию,
DocsVision