Информационная безопасность в среде EMC Documentum

В статье дано представление о механизмах защиты информации в среде EMC Documentum, большинство из которых встроены непосредственно в ее центральный компонент – Documentum Content Server (DCS). Для проектов, где требуются наивысшие уровни безопасности и контроля доступа, используются расширенные средства безопасности служб шифрации данных Documentum Trusted Content Services (интегрированные в DCS), а также – EMC Documentum IRM (Information Rights Management) – для обеспечения защиты информации за пределами репозитория.

Введение

Системы электронного документооборота (СЭД) занимают все большее место в корпоративных информационных системах в качестве универсальной платформы для интеграции и управления информацией, становясь одной из центральных компонент всей корпоративной инфраструктуры. В большинстве СЭД средства обеспечения информационной безопасности (ИБ) являются встроенными в составе приложения, но при необходимости они могут быть расширены ИБ-решениями и ИБ-технологиями, лежащими ниже уровня приложений (например, рассмотренными в SN № 3/32, 2007 – "Гетерогенное управление безопасностью данных в БД", "Безопасный доступ и хранение данных: СУБД Oracle", "Защита информации от кражи из информационных систем").

Архитектура ИБ в EMC Documentum

Архитектура ИБ в EMC Documentum является одной из наиболее продуманной и глубокой для данного класса приложений, обеспечивающей ИБ на всех этапах – доступа, передачи, хранения, использования. В общей иерархии сервисов архитектуры Documentum уровень безопасности "лежит" между уровнями сервисов репозитория и комплайнс (рис. 1). С точки зрения реализации, базовая функциональность ИБ поддерживается в составе Documentum Content Server; расширенная – на основе Documentum Trusted Content Services, а функциональность обеспечения ИБ вне репозитория – на основе EMC Documentum IRM (рис. 2).

Documentum Content Server – безопасность на уровне платформы

Большинство функций безопасности платформы встроены непосредственно в ее центральный компонент – Documentum Content Server, в частности:

– аутентификация;

– framework аутентификация;

– управление идентификацией;

– авторизация;

– контроль доступа и управление в комнатах коллективной работы EMC Documentum;

– аудит;

– шифрованная передача данных.

Аутентификация

Для получения доступа к содержанию, хранимому в хранилище Documentum, пользователи должны аутентифицироваться – доказать системе, что они являются теми, кем себя объявляют. Аутентификация по умолчанию проверяет имя и пароль пользователя, но эти данные не хранятся в Documentum. Платформа использует пароли операционной системы. Такая функциональность, как требуемый синтаксис паролей или срок их действия пароля, контролируется ОС. В дополнение к функциональности ОС, платформа Documentum обеспечивает:

- *ограничение числа попыток входа в систему во избежание "атак грубой силой" (brute force).* Атака brute force – технология взлома пароля, исполь-

Рис. 1. Место сервисов безопасности в общей иерархии уровней архитектуры EMC Documentum.

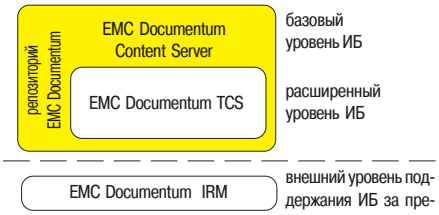

Рис. 2. Покомпонентная реализация функциональности ИБ в системе Documentum.

зующая вычислительные мощности для перебора всех комбинаций символов, из которых может состоять пароль. Количество попыток ограничивается небольшим набором (обычно тремя). При превышении этого количества учетная запись пользователя блокируется для предотвращения дальнейших попыток;

- *блокировку по превышению времени простоя.* Администраторы могут устанавливать время, по истечении которого система завершает любую неактивную сессию. Это предотвращает несанкционированный доступ к рабочей станции пользователя, который "попал в непредвиденные обстоятельства". Эта возможность обычно сочетается со скринсейвером, который запирает доступ к рабочей станции конечного пользователя;
- *возможность как внутренней, так и внешней аутентификации в режиме реального времени.* Учетные записи с параметрами доступа пользователя, предоставленные в ответ на запрос аутентификации, могут в режиме реального времени проходить внутреннюю проверку в Documentum Content Server или внешнюю — в службе каталогов. Эта возможность позволяет платформе Documentum включиться в корпоративную инфраструктуру управления идентификацией (Identity Management);
- *аудит попыток входа в систему в журнале аудита Content Server.* Подобно любому действию любого пользователя с любым объектом в системе Documentum, все попытки аутентификации, как успешные, так и неудачные, отслеживаются в центральном журнале аудита. Данный аудиторский след позволяет в последующем осуществлять анализ всех вопросов, связанных с аутентификацией.

Framework аутентификация

Аутентификация Documentum Content Server основана на открытой архитектуре, которая может использовать дополнительные средства аутентификации, помимо имени и пароля пользователя, использование которых происходит по умолчанию. Framework аутентификации Documentum позволяет подключать внешнюю проверку аутентификации, принцип единой регистрации (Single Sign-on – SSO) и многофакторную аутентификацию, а также поддерживает различные возможности расширения системы безопасности, такие как биометрика, сертификаты X509.3 – инфраструктуру открытых ключей (PKI), токены и смарт-карты.

Управление идентификацией

Платформа Documentum предназначена для бесшовной интеграции с корпоративной ИТ-инфраструктурой, включая управление идентификацией корпоративного уровня (Enterprise Identity Management). Documentum Content Server поддерживает одновременное соединение с несколькими службами каталогов и обеспечивает интеграцию с такими каталогами предприятия, как:

- Microsoft Active Directory;
- Sun ONE Directory Server;
- Oracle Internet Directory;
- IBM Tivoli Directory Server;
- Novell eDirectory;
- Microsoft ADAM.

Службы доступа к каталогам реализуются посредством стандартного протокола LDAP (Lightweight Directory Access Protocol). Интеграция позволяет осуществлять синхронизацию пользователей и групп в масштабе всего предприятия. Администраторам Documentum нет необходимости индивидуально заводить каждого пользователя и группу в Documentum Content Server, что при наличии тысяч пользователей может стать утомительной задачей. Упрощение и централизация управления пользователями и группами повышает безопасность всех вовлеченных в этот процесс систем, а децентрализованное управление, напротив, приводит к уязвимости, вследствие несоответствий между системами и повышения вероятности ошибки администратора.

Синхронизация пользователей и групп пользователей с каталогом происходит через регулярные интервалы, установленные администратором. При необходимости администратор также может инициировать мгновенную синхронизацию. Для администрирования нескольких каталогов используется объединенная модель, поддерживаемая платформой Documentum. Объединенное администрирование обеспечивает центральную точку контроля для географически распределенной системы Documentum. В результате затраты на администрирование могут быть значительно снижены.

Шифрованная передача данных

С использованием протокола защиты Secure Sockets Layer (SSL) все данные, пересылаемые между Documentum Content Server и клиентскими приложениями, включая Documentum Desktop и любое приложение на основе WDK, например, Documentum Webtop, могут быть зашифрованы. Дополнительно с помощью SSL можно зашифровать данные, передаваемые между сервером Documentum Content Server и службами каталогов. Documentum Content Server может быть настроен на использование защищенных или незащищенных портов, и клиентам может быть разрешено соединение только через защищенные порты (рис. 3). Documentum SSL для обмена ключами использует алгоритм ADH (Anonymous

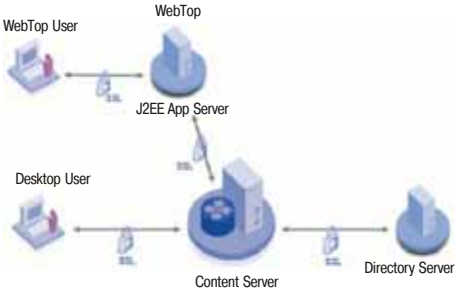

Рис. 3. Секретность данных, обеспечиваемая связью с шифрацией с использованием SSL.

Diffie-Hellman – алгоритм шифрования с открытым ключом, Диффи-Хельмана) с размером ключа 1024 бит. При шифровании данных используется алгоритм AES с 256-битными ключами.

Шифрованная связь предотвращает перехват и гарантирует секретность данных. Она увеличивает гибкость сетевой архитектуры и позволяет службам каталогов или Documentum Content Server находиться внутри или вне демилитаризованной зоны (DMZ).

Дополнительная ИБ с использованием служб шифрации данных EMC Documentum Trusted Content Services

Службы шифрации данных EMC Documentum Trusted Content Services (TCS) являются опциональным продуктом, который обеспечивает дополнительный уровень безопасности и дополняет функции безопасности Documentum Content Server. TCS глубоко встроены в Documentum Content Server и их возможности могут быть задействованы при помощи соответствующего лицензионного ключа.

TCS позволяют организовать надлежащую защиту информационных активов даже организациям с высочайшими требованиями к безопасности. Возможности, предоставляемые TCS, включают:

- шифрование хранилищ;
- электронные подписи;
- мандатный контроль доступа (MAC);
- цифровое уничтожение (электронный шреддинг).

Шифрование хранилищ

TCS позволяет осуществлять шифрование файловых хранилищ, в которых хранятся объекты содержания в репозитории Documentum. Шифрование файлового хранилища предотвращает доступ к файлам содержания на уровне операционной системы. Например, если злоумышленники смогут отключить защиту уровня ОС, то все что они увидят – зашифрованные файлы. Данный тип защиты предотвращает злонамеренные нарушения защиты изнутри, например, со стороны администратора.

Шифрование в файловом хранилище может применяться селективно, что позволяет иметь зашифрованные и незашифрованные файлы в одном и том же репозитории, обслуживаемом одним и тем же Documentum Content Server. В TCS используется алгоритм шифрования 3DES-CBC с длиной ключа 192 бит. EMC лицензирует все алгоритмы шифрования у компании RSA Security (приобретена EMC в 2006 г. за $2,2 млрд).

Шифрование происходит внутри Documentum Content Server "ниже уровня интерфейсов API", что означает, что содержание представляется через Documentum API в незашифрованной форме. Все приложения осуществляют доступ к зашифрованному содержанию без декодирования — таким образом, будто никакого шифрования не применялось. Шифрование не влияет на индексирование и полнотекстовый поиск.

Шифрование репозитория также применяется ко всем резервным копиям, созданным на уровне файловой системы. В результате можно безопасно хранить носители резервных копий без риска нарушения их защиты. Приложение EMC Legato NetWorker для Documentum, например, позволяет осуществлять резервное копирование и восстановление зашифрованных файлов с резервных лент, содержащих зашифрованные данные.

Шифрование хранилища применяется только к файлам содержания, а не к его метаданным (атрибутам содержания). Тем не менее, поскольку метаданные хранятся в стандартной реляционной базе данных, можно использовать любые инструменты безопасности РСУБД, предоставленные поставщиком БД. Oracle, например, предоставляет полное решение для шифрования БД.

Любое шифрование снижает уровень производительности. Измеренное уменьшение производительности Documentum Content Server при использовании шифрования составляет менее 12%. Любое другое уменьшение производительности, вызванное журналами аудита, выполнением методов и другими событиями, является пренебрежимо малым. Преимущества безопасности TCS, однако, являются весьма значимыми:

- безопасность содержания даже при нарушении защиты ОС;
- защита от "злонамеренного" администратора;
- безопасность отдельного хранения резервных копий;
- безопасная утилизация резервных копий.

Электронные подписи

TCS позволяет подписывать электронной подписью любой объект содержания или любое событие содержания, например, задание в бизнес-процессе. Электронные подписи защищенным образом связаны с объектом содержания и хранятся в хранилище Documentum в составе журнала аудита. Любое последующее изменение содержания делает хранимую подпись недействительной.

Подписи имеют отметку даты и времени и содержат имя и пароль подписавшего лица, а также обоснование подписи. Каждая подпись содержит контрольную хеш-сумму, которая проверяет аутентичность подписанного содержания. Допуск для ввода электронной подписи получают только уполномоченные пользователи. В процессе подписи можно сделать обязательным использование кодов обоснований, соответствующих требованиям FDA 21 CFR, часть 11. В соответствии с этими требованиями подпись должна быть видимой при просмотре и печати документа. Это требование может быть выполнено с помощью средств управления PDF, которые сличают набор строк, представляющих подписи с шаблоном, определяющим, где необходимо разместить эти подписи.

Платформа Documentum также обеспечивает основу для использования цифровых подписей, применяемых в качестве юридического доказательства подлинности документов. Цифровая подпись представляет собой элемент данных, который позволяет получателю сообщения или транзакции удостоверить подлинность ее содержания и личность подписавшего. Она является электронным эквивалентом наличия подписанного и нотариально заверенного бумажного документа, но не является цифровым образом подписи, произведенной вручную ("чернильной подписи"). Подлинность подписи удостоверяется методом строгой аутентификации (то есть, PKI-криптографией), а не сочетанием имени/пароля пользователя. Цифровые подписи являются переносимыми и могут быть удостоверены за пределами организации или местоположения подписавшего лица. Когда пользователи решают поставить "цифровую подпись" на документе, им предоставляется интерфейс, отображающий "законодательное уведомление", раскрывающийся список обоснований для выполнения выбранного действия и удостоверяющая форма пользователя.

Цифровое уничтожение

Физически во время стандартной процедуры удаления файла удаляется только информация из оглавления файловой системы, означая тем самым, что место занимаемое файлом, теперь свободно. При этом информация самого файла остается на диске. И даже после однократной перезаписи удаленные файлы могут быть восстановлены путем анализа магнитных следов, которые данные оставляют после себя на средстве хранения.

Цифровое уничтожение (электронный шреддинг) навсегда уничтожает данные файлов при совершении команды удаления/отмены связи. Система автоматически несколько раз производит перезапись в место бывшего хранения данных, чтобы гарантировать невозможность их восстановления, даже путем анализа остаточного магнетизма. Данная функция TCS поддерживает приложения, обеспечивающие регламенты хранения и управление записями, которые определяют, в какой момент в ходе жизненного цикла содержания следует производить утилизацию. Платформа Documentum обеспечивает цифровое уничтожение содержания, хранящегося в файловых системах, а также в адресуемом хранилище содержания, основанном на решении EMC Centera. Цифровое уничтожение считается обязательным шагом для большинства приложений управления записями.

EMC Documentum IRM – управление правами на информацию вне репозитория Documentum

Выше были рассмотрены вопросы, связанные с защитой информации внутри репозитория (или хранилища) документов. Однако в настоящее время все более очевидным становится то, что в случае извлечения из репозитория (внутри которого реализованы самые передовые технологии информационной безопасности) документа, содержащего конфиденциальный контракт или план выпуска продукта, он может быть рассекречен после того, как он был открыт на рабочей станции, отправлен по почте или распечатан. За пределами хранилища никакие регламента контроля за доступом или разграничений прав на работу с документами не действуют! Кроме того, к этому же классу рисков можно отнести ситуации, когда пользователь открывает сохраненную "про запас" на своем локальном компьютере устаревшую версию документа. Поэтому важной задачей становится обеспечение безопасности содержания с того момента, как оно покидает репозиторий. Эта область является сферой деятельности технологий цифрового управления правами (Digital Rights Management, DRM), также называемых управлением правами на информацию (Information Rights Management, IRM).

DRM обеспечивает возможность расширения управления содержанием за пределы репозитория. Documentum IRM позволяет определять привилегии доступа внутри репозитория Documentum и за его пределами.

В Documentum IRM большое внимание уделено тому, чтобы обеспечить защиту взаимодействия клиента с сервером, предотвратить прямой доступ к ключам шифрования и незашифрованному тексту, а также контролировать все разрешенные действия с информацией после того, как она дешифрована и представлена пользователю. Результатом этих усилий является постоянный контроль, который открывает существенно новые возможности в отношении способов использования секретной информации.

Для электронной защиты информации Documentum IRM Server использует криптографию. Используется несколько шифров с различной длиной ключа. Шифр — это формула, которая сначала применяется к незашифрованному тексту (информации) для того, чтобы получить закодированный текст (зашифрованную информацию), а затем инвертируется, чтобы получить незакодированный текст из закодированного текста. В качестве переменной функции обычно используется "ключ". В этом документе не обсуждаются сами криптографические ключи и то, как они работают. Однако мы хотели бы упомянуть о том, что криптографические алгоритмы в основном относятся к одной из двух категорий: с симметричным или с асимметричными шифром. Говоря "симметричная криптография", обычно имеют в виду такой способ шифрования, когда для шифрования и дешифрования используется один и тот же ключ. Выражение "асимметричная криптография" обычно означает, что используется пара ключей — один для шифрования, а другой для дешифрования информации (например, данные кодируются при помощи ключа А, а декодируются при помощи ключа Б). Documentum использует симметричный ключ для защиты информации в документах и сообщениях. Таким образом, один и тот же ключ используется и для шифрования, и для дешифрования информации. Для получение более подробной информации о криптографии рекомендуем обратиться к книге "Прикладная криптография" Брюса Шниера (ISBN 0-471-11709-9).

Архитектура Documentum IRM

Архитектуру Documentum IRM составляет семейство клиентских приложений или плагинов, которые взаимодействуют с общим сервером политик, для того чтобы защищать и контролировать электронную информацию. Каждое из клиентских приложений отвечает за работу с определенным типом или форматом информации. Например, Documentum IRM Client for Microsoft Office является COM-дополнением для приложений Microsoft Office (особенно для Word, Excel и PowerPoint), спроектированным для защиты и контроля над документами этих форматов. Плагин Documentum IRM Client for Adobe Acrobat создан для защиты и контроля PDF-документов. Аналогично, Documentum IRM Client for eRoom является набором плагинов для различных e-mail-клиентов, таких, как Outlook и Lotus Notes, направленных на защиту сообщений электронной почты. Когда владелец информации желает защитить и контролировать ее, он должен начать с регистрации этого содержания в помощью Documentum IRM Server (шаг 1, рис. 4). Регистрацию можно запустить из того приложения, в котором создано содержание (такого как Office, Outlook или

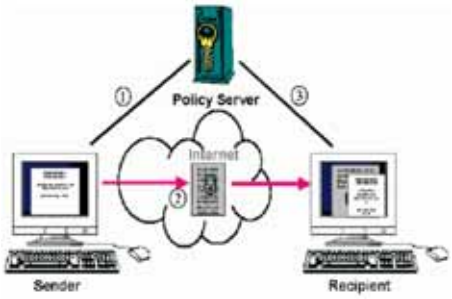

Рис. 4. Процедура использования защищенного контента: шаг 1 – устанвление защищенного соединения с сервером политик; шаг 2 – передача зашифрованного контента; шаг 3 – аутентификация получателя и запрос ключа для дешифрации документа.

Acrobat). Однако, как правило, заказчики Documentum выполняют это действие в пакетном режиме и еще более часто — в программном, поскольку эти средства защиты наиболее часто используются в крупномасштабных приложениях для совместного использования содержания. Оба режима — регистрация, инициируемая пользователем, и программная регистрация одинаково хорошо поддерживаются. В результате инициации процесса регистрации плагин Documentum IRM устанавливает защищенное соединение с сервером политик. Пользователь или программный процесс после аутентификации сервером политик выбирает желаемые параметры защиты (например, кто может получить доступ к содержанию, можно ли его печатать, нужно ли накладывать на него водяные знаки, должно ли оно автоматически самоуничтожиться в какой-то момент будущего времени и т.п.). Затем Documentum IRM Server случайным образом генерирует ключ шифрования для каждой страницы содержания, записывает локальную копию ключа и политик и отправляет ключ клиентскому приложению. Клиентское приложение шифрует каждую страницу документа с использованием соответствующего ключа, применяя симметричный шифр (256-разрядный AES[1]), а затем уничтожает его. По завершении процесса в Documentum IRM Server остаются только политики и ключи шифрования документа. На клиентской же машине остается только зашифрованное содержание — пользователю не доступны ни ключи, ни исходный текст.

После того, как содержание зарегистрировано, его можно безопасно распространять через наиболее подходящий механизм или протокол (шаг 2, см. рис. 4). Когда содержание защищено само по себе, нет необходимости использовать защищенное соединение. Однако некоторые заказчики для повышенной защиты используют защищенное соединение для пересылки содержания.

В тот момент, когда получатель пытается открыть защищенное содержание, автоматически вызывается соответствующий клиентский плагин Documentum IRM. Плагин снова устанавливает защищенное соединение с Documentum IRM Server, где хранятся ключи дешифрации (шаг 3, см. рис. 4). Через это соединение происходит аутентификация получателя и делается запрос ключа для дешифрации документа. Если Documentum IRM Server определит, что доступ следует авторизовать (например, если авторизован пользователь, выполнены все ограничения временного окна, запрос пришел с авторизованного IP-адреса и т.д.), он посылает плагину через защищенное соединение ключ и применяет ограничения (можно ли копировать или печатать, какие водяные знаки должны появиться и т.д.). Плагин, ограничивая возможности клиентского приложения для просмотра, расшифровывает содержание, формирует его экранное изображение, а затем немедленно уничтожает дешифрованное содержание и полученные копии ключа. Для защищенных PDF-файлов при переходе пользователя к следующей странице формируется запрос на следующий ключ. Владелец информации в любой момент времени может аннулировать доступ данного пользователя к документу или изменить применяемые ограничения. Эти изменения будут применены к защищенным документам MS Office и сообщениям электронной почты в момент их следующего открытия, изменения же для защищенных PDF-файлов вступают в действие немедленно. При удалении ключей из Documentum IRM Server — вручную владельцем информации или автоматически по истечении срока хранения, все копии документа будут подвергнуты цифровому уничтожению. Это возможно благодаря тому, что клиентское приложение никогда не хранит локальные копии ключей (за исключением обсуждаемого ниже случая, когда разрешено офлайновое владение документом).

Начиная с того момента, как доступ к защищенной информации вызывает взаимодействие с Documentum IRM Server для аутентификации, сервер обеспечивает расширенный аудиторский контроль. Благодаря журналу аудита, владельцы информации могут определить, кто и к какому документу получал доступ, когда и с какого IP-адреса, распечатывался ли документ (в случае разрешенного вывода на печать).

Documentum IRM Server — это служба, которая принимает соединения от различных клиентов, аутентифицирует пользователей, обеспечивает авторизацию и передачу ключей шифрования и применяет политики к защищенному содержанию. Система основана на том, что никто, даже авторизованные пользователи, не могут получить прямой доступ к ключам шифрования. Для этой цели ключи шифрования и другая секретная информация также шифруется на время хранения в базе данных сервера. Что же касается ключа шифрования, то это секретное значение генерируются случайным образом, когда инициализируется Documentum IRM Server, и хранится в конфигурационном файле сервера authentica.cfg. Помимо базы данных ключей шифрования, еще некоторая конфигурационная информация, часть из которой является секретной, хранится в конфигурационном файле сервера. Например, в файле authentica.cfg хранятся публичные и приватные ключи[2] сертификата сервера, используемые для аутентификации сервера и установления защищенного соединения с клиентами. Когда “все ключи от королевства” лежат в одном файле, что может защитить этот файл? Идентификационная фраза для запуска сервера используется в качестве компонента для того, чтобы вычислить ключ для дешифрования секретной информации, хранимой в файле authentica.cfg. При старте сервер запрашивает у администратора идентификационную фразу. Сервер использует идентификационную фразу для того, чтобы открыть файл authentica.cfg и извлечь необходимую информацию. После этого сервер становится в режим ожидания соединений с клиентами.

Защита сессий

Documentum IRM Server на основе политики выделяет ключ шифрования удаленному клиенту, когда этот клиент соединяется с сервером и запрашивает ключ. Такое соединение и взаимодействие осуществляется через сессию зашифрованной коммуникации. Эта сессия защищена с использованием двух уровней шифрования. Когда клиент устанавливает соединение с сервером, запускается SSL-сессия — точно так же, как при соединении с https-сайтом. SSL использует по крайней мере один сертификат сервера для аутентификации взаимодействующих сторон и генерации ключа шифрования сессии. В рамках данного документа не рассматривается, как действует SSL, но это обсуждается на веб-сайтах разработчиков Netscape2. Ключ сессии генерируется случайным образом, это 168-разрядный тройной DES-ключ.

1) Advanced Encryption Standard, улучшенный стандарт шифрования, принят Министерством торговли США 12 октября 2000 г. вместо устаревшего стандарта DES. Стандарт симметричного блочного шифрования (длина блока -128 бит) AES поддерживает 128-разрядные ключи, но может поддерживать более длинные, 192- и 256-разрядные. Базируется на алгоритме Rijndael (читается "рейн-долл"), разработанном бельгийскими криптографами Джоаном Дименом и Винсентом Риджменом.

2) Публичный и приватный ключи играют роль асимметричной криптографии. Сертификаты в основном используют асимметричную криптографию.

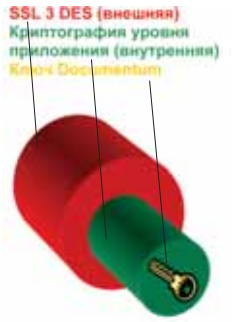

Рис. 5. Защита сессий в среде Documentum IRM.

Одна из задач системы Documentum IRM – предотвращение прямого доступа к ключам дешифрования и секретной информации — даже для пользователей, авторизованных для просмотра содержания. Являясь авторизованным пользователем и обладая специальными знаниями, используют также второй 128-разрядный ключ сессии для шифрования данных на уровне приложений, что создает второй туннель шифрования внутри SSL-туннеля (рис. 5).

Отделение ключей от содержания

Многие системы, которым приходится осуществлять контроль над информацией после ее распространения, используют такой подход, при котором ваучер с криптографическим ключом предоставляется пользователю после того, как он аутентифицирован или выполнил определенную операцию, такую, как оплата за контент. Эти системы берут ключи и опции политик и шифруют их в ваучер, который хранится в системе получателя. Клиентское приложение для просмотра использует один из “секретных” алгоритмов, чтобы дешифровать ваучер, достать из него ключ, а затем расшифровать содержание и применить политику. Одним из недостатков этих систем является то, что злоумышленник может произвести офлайновую атаку и обнаружить секретный алгоритм. Как только такой пользователь обнаружит этот алгоритм, он сможет генерировать и распространять свои собственные приложения, которые будут взламывать все защищенное по данной схеме содержание. Известны несколько примеров подобного развития событий. Другим недостатком этого подхода является то, что после того, как пользователю предоставлен ваучер, не существует надежного способа изменить или аннулировать его доступ. Получатель всегда сможет сделать копию состояния системы и воспроизводить это состояние в будущем, когда захочет получить доступ к информации.

Documentum IRM использует другой подход. Хранение ключа и информации о политиках только на сервере предотвращает офлайновые атаки. Более того, вам не нужно полагаться на секретный алгоритм для защиты ваучера. В схеме, применяемой в Documentum, все решения, основанные на времени, базируются на часах сервера (а не на часах локального клиента), которые не могут стать объектом манипуляций пользователя-злоумышленника.

Заключение

В современных распределенных корпоративных IT-инфраструктурах законченные системы обеспечения безопасности информационных систем могут быть реализованы только на основе многоуровневых решений, поддерживающих правила доступа, передачи, хранения и использования информации глобально, на заданном уровне требований и на всех этапах обработки документов.